UNIVERSIDAD DE PANAMA
VICERRECTORIA DE INVESTIGACIÓN Y POSTGRADO
FACULTAD DE INFORMATICA Y COMUNICACIONES
UNIVERSIDAD CARLOS III DE MADRID

GUIA PARA LA IMPLEMENTACIÓN DE UN PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP) PARA EL IFARHU PANAMA

ROBERTO CHAN

ASESORES
DR BENJAMIN RAMOS ALVAREZ
DRA ALMUDENA ALCAIDE

TESIS PRESENTADA COMO UNO DE LOS REQUISITOS PARA OPTAR AL GRADO DE MAESTRIA EN GESTIÓN Y TECNOLOGIA DEL CONOCIMIENTO

PANAMA REPUBLICA DE PANAMA
2013

18 MAR 2014

UNIVERSIDAD DE PANAMÁ
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO
DIRECCIÓN DE POSTGRADO

VIP-DP--12
17 de enero de 2013

Ingeniera
Amarilis De León
Coordinadora
Maestría en Gestión y Tecnología del Conocimiento
Facultad de Informática, Electrónica y Comunicación
Universidad de Panamá
E. S. D.

Estimada Señora Coordinadora:

Atendiendo su solicitud de inscripción del Proyecto de Intervención, adjunto copia de la misma con su respectivo código para los trámites pertinentes.

NOMBRE DEL ESTUDIANTE	TÍTULO DEL PROYECTO	CÓDIGO
José Guillermo	Evaluación del Entorno Organizacional para la Implementación de un Plan de Recuperación de Desastres de Tecnología en la AIG- Análisis de Impacto al Negocio.	CE-PI-327-17-03-13-01
Erasmo Cedeño	Guía para el Desarrollo de un Plan de Recuperación de Desastres (DRP) para el IFARHU, Panamá.	CE-PI-327-17-03-13-02
Roberto Chan NG	Guía para la Implantación de un Plan de Recuperación ante Desastres (DRP) para el IFARHU, Panamá	CE-PI-327-17-03-13-03
Gustavo Chery	Diseño de un BPM (Business Process Management) o Gestión de procesos de Negocios a través de un Bus de Servicio Empresarial SOA (Arquitectura Orientada	CE-PI-327-17-03-13-04
Lastenia Degracia Murillo	Estrategia de Inteligencia de Negocios.	CE-PI-327-17-03-13-05

CIUDAD UNIVERSITARIA OCTAVIO MÉNDEZ PEREIRA
Estafeta Universitaria, Panamá, República de Panamá
Tels.: (507) 523-5320 Fax: (507) 523-5310
Correo electrónico: upvipdp@ancon.up.ac.pa

Benilda Paz	Una VDI con enfoque de Inteligencia de negocio: un caso práctico.	CE-PI-327-17-03-13-16
Maribel Wong	Eficiencia en los Municipios Panameños utilizando herramientas de Gobierno Electrónico.	CE-PI-327-17-03-13-17
Miguel Ángel Zelada M.	Diseño de arquitectura orientada a servicio a través de un Bus de Servicio Empresarial.	CE-PI-327-17-03-13-18
Armando Zurita	Sistemas Inteligentes para la reducción del hacinamiento carcelario, basado en la clasificación de privados de libertad, mediante el uso de brazaletes y el desarrollo de la video audiencias.	CE-PI-327-17-03-13-19

Atentamente,

Dr. Filiberto Morales
Director de Postgrado

Adj. lo indicado

/bed

CIUDAD UNIVERSITARIA OCTAVIO MÉNDEZ PEREIRA
Estafeta Universitaria, Panamá, República de Panamá
Tels.: (507) 523-5320 Fax: (507) 523-5310
Correo electrónico: upvipdp@ancon.up.ac.pa

UNIVERSIDAD DE PANAMÁ
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

ACTA DE SUSTENTACIÓN
DEL PROYECTO DE INTERVENCIÓN

SEDE: Facultad de Informática, Electrónica y Comunicación

PROGRAMA DE MAESTRÍA EN: Gestión y Tecnología de del Conocimiento

Título del Proyecto de Intervención: Guía para la implementación de un Plan de Recuperación Ante Desastres (DRP) para el IFARHU, Panamá.
Nombre del Participante: CHAN NG, ROBERTO
CIP Nº: 8-382-627

Miembros del Jurado: **Calificación otorgada:**

NOMBRE Y FIRMA DE LOS MIEMBROS DEL JURADO		TRABAJO ESCRITO	DEFENSA	PROMEDIO
NOMBRE	FIRMA			
DR. AGAPITO LEDEZMA		46	46	92
DR. ANGEL GARCIA OLAYA		46	45	91
DR. IVAN ARMUELLES VOINOV		46	48	94
			NOTA FINAL	92,3

Recomendaciones del Jurado:
Corregir errores gramaticales en el Documento final.

Firma del Director de Investigación y Postgrado o Coordinador del Programa

Firma del Representante de la VIP

Firma del Estudiante: Roberto Chan

Fecha: 29/11/2013

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ABREVIATURAS

AIG: Autoridad para la Innovación Gubernamental.

ASE: Asesor de Seguridad.

BIA: Business Impact Analysis.

BCI: Business Continuity Institute.

CD: Compact Disk.

COBIT: Control Objectives for Information and related Technology.

CIT: Coordinador de Infraestructura Tecnológica.

CRTI: Coordinador de Recuperación de TI.

DRII: Disaster Recovery Institute International.

DRP: Disaster Recovery Plan.

IFARHU: Instituto para la Formación y Aprovechamiento de los Recursos Humanos.

ITIL: Information Technology Infrastructure Library.

MTD: Maximun Time Down.

NIST: National Institute of Standards and Technology.

RPO: Recovery Point Objective.

RTO: Recovery Time Objective.

SAN: Storage Area Network.

TI: Tecnología de la Información.

TIC: Tecnología de la Información y Comunicaciones.

USB: Universal Serial Bus.

UPS: Uninterruptible Power Supply.

WRT: Work Recovery Time.

RESUMEN

El presente documento tiene como finalidad revisar el estado actual de la infraestructura tecnológica en que se apoya los servicios brindados por el IFARHU, también evaluar los riesgos y procedimientos a seguir en caso de presentarse alguna situación anormal o contingencia. La metodología empleada en el documento incluye una encuesta en las diversas áreas dentro de nuestra organización, de allí se establece una evaluación de los servicios prioritarios para mantener las operaciones mínimas requeridas por la organización en caso de presentarse una contingencia. También analizamos los eventos más comunes por los diferentes riesgos tanto internos como externos y las amenazas naturales ocurridos en nuestro país, y que pueden afectar nuestra atención a los estudiantes; con la información antes mencionada y el inventario tanto del hardware como software sirve como entrada para el Análisis de Impacto del Negocio (BIA). Analizaremos diferentes alternativas o soluciones ante estos eventos o contingencia, sus ventajas y desventajas; todo esto dependerá de las políticas establecidas dentro de las estrategias para mantener la continuidad del negocio. En este documento, presentamos una guía para la implementación de un Plan de Recuperación ante Desastres (DRP) para el IFARHU desde la concepción o definición del mismo como un proyecto, el equipo interdisciplinario que lo debe conformar para lograr el éxito de la misma en las diferentes etapas, así como las diferentes tareas, objetivos y entregables dentro de cada fase.

SUMMARY

This document is intended to review the current state of the technology infrastructure that supports the services provided by IFARHU, also evaluate the risks and procedures to follow in case of any abnormal condition or contingency. The methodology used in this paper includes a survey of the different areas within our organization, hence provides an assessment of priority services to maintain minimal operations required by the organization in the event of a contingency. We also analyze the most common events through the different internal and external risks and natural hazards occurring in our country, and that may affect our attention to students; with the above information and inventory of both hardware and software is used as input to the Business Impact Analysis (BIA). We analyze different alternatives or solutions to these events or contingencies, their advantages and disadvantages, all this will depend on the policies established in strategies to maintain business continuity. In this paper, we present a guide to the implementation of a Disaster Recovery Plan (DRP) for IFARHU from conception or definition of it as a project, the interdisciplinary team that must conform to the success of it in the different stages and different tasks, objectives and deliverable within each phase.

INTRODUCCIÓN

En la actualidad, podemos observar cada vez más frecuente la ocurrencia de desastres naturales como terremotos, tormentas tropicales, maremotos, erupciones volcánicas, etc., los cuales pueden afectar en grandes dimensiones a una área geográfica como a una nación entera. Estos desastres pueden afectar en forma directa o indirectamente, por ejemplo, los efectos de una tormenta tropical que puede provocar la caída del tendido eléctrico y esto afectar por horas o días el levantamiento de este servicio. Por lo mencionado, podemos observar que es común poner en práctica procedimientos o acciones a seguir en caso de un evento como este en nuestros hogares, tal como contar con linternas, baterías, plantas eléctricas, etc., dependiendo del desastre natural ocurrido y la magnitud. En áreas donde ocurren muchos huracanes, es común que se organizan y tienen áreas de refugios donde ya se encuentra establecido por parte del gobierno planes de ayuda y distribución de los alimentos, agua y medicina para la población afectada.

En este trabajo, vamos a enfocarnos en los procedimientos o acciones a seguir en caso de que ocurra un desastre natural que pueda afectar los servicios que brinda nuestra organización o empresa. Con la utilización de las primeras computadoras para el procesamiento de datos en lo que considerábamos como un gran volumen en sus tiempos y con el pasar de los años, hemos ido observando cómo ha evolucionado el mundo de la informática con los avances de las tecnologías. En Panamá, podemos recordar tanto en la empresa privada como gubernamental se inicia como un Centro de Procesamiento de

Datos y por lo general estaba dirigida por Finanzas debido al gran volumen de transacciones que debían procesar.

Hoy en día, muchos de estos Centro de Procesamiento de Datos han sido elevados a nivel de Gerencia o Dirección de Informática, tal como es el caso en el IFARHU que pasa de Oficina de Informática a Dirección de Tecnología Informática a finales de noviembre del 2007. Con esto crea una mayor autonomía y participación de los profesionales en al área de informática para el apoyo en la toma de decisiones por parte de los altos ejecutivos dentro de una organización o empresa, basados en los sistemas de información. Estos sistemas están compuestos por una serie de componentes desde las aplicaciones, la base de datos, los servidores, las redes, el cableado, etc., para que los usuarios tengan acceso a estos desde diferentes áreas geográficas y son las mismos que deben tomar sus decisiones basados en la información; por ejemplo, decisiones apoyado en la información y el modelo a utilizar que nos ayude a pronosticar las tendencias futuras, y así solicitar el presupuesto requerido o necesario en el otorgamiento de nuevas becas escolares y préstamos educativos, como es el caso nuestro en el IFARHU.

Como pueden observar, el uso de la tecnología no sólo se centra como herramienta para unos cuantos departamentos sino que en la actualidad son un gran apoyo en toda la organización. Por lo antes mencionado, es importante destacar la necesidad de la disponibilidad, confiabilidad y continuidad de estos servicios a nivel de la organización; esto conlleva que el profesional del área de informática debe ir actualizando y poner en marcha las mejores prácticas para mantener las operaciones continuas de estos recursos.

En este trabajo hacemos mención de puntos importantes a considerar o factores que deben tomar en cuenta para la implementación de un Plan de Recuperación ante un

Desastre (Disaster Recovery Plan - DRP) por amenazas naturales en Panamá, específicamente para el área de la Dirección de Tecnología Informática, la cual no es más que los pasos o acciones a seguir ante una situación de desastre para la rápida recuperación ante estos hechos. Esto tiene como finalidad poner en práctica no solamente las acciones a ejecutar cuando ocurre el desastre, sino también como evitar o mitigar los riesgos para minimizar el tiempo de interrupción de los servicios prestados.

Además del DRP, debemos hacer mención de otro concepto importante que es el Plan de Recuperación del Negocio (Business Recovery Planning – BRP), el cual va más allá del DRP que además del procesamiento de datos, también está enfocado en la recuperación de las operaciones del resto de la organización aunque no vamos a entrar en detalle sobre este tema. Para la elaboración del DRP, debemos tener en cuenta otro tema importante que es el Plan para Continuidad del Negocio (Business Continuity Plan – BCP)[1], el cual abarca tanto del DRP como el BRP y que nos servirá de guía ya que debemos considerar los indicadores y las prioridades establecidas por la organización, como los tiempos de respuestas, los servicios prioritarios o críticos, respaldo de los sistemas, seguridad física y lógica, etc.

Este trabajo tiene como objetivo servir de guía para la implementación del DRP del IFARHU desde la fase inicial, debido a que actualmente no cuentan con un plan de acción o los procedimientos no están claramente establecidos y documentados.

Actualmente, más de 600,000 estudiantes depende de los servicios ofrecidos por el IFARHU para realizar sus estudios a nivel de Básica General, Media y universitario

---

[1] *Business Continuity and Disaster Recovery Planning, in The Official (ISC) 2 CISSP CBK Review Seminar*, Student Handbook, Version 12.0. [Massachusetts, USA]: High Stakes Writing, 2011. Página II-1 - II-36.

como Carreras Técnicas, Licenciaturas, Postgrados y Maestrías; la mayoría de los estudiantes se encuentran a nivel nacional y una minoría realiza sus estudios a nivel superior en el extranjero. Todos estos estudiantes que realizan sus estudios ya sea por medio de una beca o de un préstamo educativo, depende que el IFARHU le haga llegar el recurso económico para poder continuar con sus estudios en los diferentes centros educativos, por lo tanto es importante mantener la disponibilidad y transparencia de los servicios ofrecidos y la continuidad del negocio por parte de esta institución.

ESTADO DEL ARTE

Este proyecto tiene como objetivo elaborar una guía para la implementación del Plan de Recuperación ante Desastres para los Sistemas de Información críticos del IFARHU, para esto debemos conocer a fondo todo lo que involucra, los pasos o fases, la información a recopilar, personal requerido, etc., todo esto con la finalidad de mantener la disponibilidad, confiabilidad y continuidad del negocio dentro de nuestra organización. Para cumplir con este propósito, vamos a realizar una búsqueda y recopilar información de diferentes fuentes a través del Internet, donde podemos examinar el tema a tratar por medio de bibliografías, monografías, artículos relacionados, investigaciones realizadas, etc.

La intención de este documento es que pueda ser utilizado como una guía o referencia, ya sea por la Dirección de Tecnología Informática o cualquier otro personal con ciertos conocimientos para seguir las etapas o fases necesarias para poder desarrollar la implementación de un DRP para el IFARHU como un proyecto. Este documento guarda una estrecha relación con otro trabajo a presentar, pero enfocado como una guía para el desarrollo del Plan de Recuperación ante Desastres para los Equipos Críticos del centro de cómputo del IFARHU.

De acuerdo a la información recopilada, el estado del arte de este trabajo sobre el DRP estará basado según la metodología de acuerdo a las recomendaciones del NIST (National Institute of Standards and Technology), del DRII (Disaster Recovery Institute International) y del BCI (Business Continuity Institute). También nos apoyaremos en

casos prácticos de estudios para el desarrollo de planes de recuperación ante desastres encontradas en diferentes medios como publicaciones, libros, manuales, etc.

Durante esta etapa del proyecto o trabajo de investigación, podemos observar que el Plan de Recuperación ante Desastres está compuesto por una serie de etapas o fases que detallamos a continuación:

- **Conceptualización:** Esta etapa tiene como finalidad definir el alcance, los objetivos, el personal necesario o requerido para las diferentes etapas durante el desarrollo, administración y aprobación del DRP, ante la ocurrencia de diversos desastres por amenazas naturales en Panamá.
- **Diseño del Plan:** Tiene como finalidad levantar el registro o inventario tanto de los equipos, como los sistemas de información que integra la plataforma tecnológica de la organización. Con esto podemos evaluar, identificar y clasificar el grado de criticidad de los sistemas de información y sus dependencias, como los requerimientos necesarios de procesamiento de los equipos y otros componentes o software requeridos.
- **Seguridad la información:** Está relacionado con la seguridad física y lógica de la información, tanto de los sistemas de información como de los equipos críticos.
- **Respaldo de los sistemas:** Se refiere al respaldo de las aplicaciones, base de datos, configuraciones y su frecuencia o periodicidad, prueba de integridad y su recuperación en equipos o sitios alternos.
- **Implementación y control del DRP:** Consiste en poner en marcha el plan establecido, las pruebas realizadas y los resultados obtenidos, así como el

mantenimiento del mismo DRP mediante la modificación y/o actualización constante e inclusión de nuevos procedimientos.

Hay que destacar que el Plan de Recuperación ante Desastres (DRP) guarda estrecha relación con el Plan de Continuidad del Negocio (BCP), pues haremos mención de uno de los aspectos más importante a considerar para la elaboración o desarrollo del DRP que es el Análisis de Impacto en el Negocio (BIA) y esto conlleva a la evaluación de riesgos. Esto no es más que la identificación de diversos eventos, que pueden afectar los sistemas de información críticos y por ende la continuidad del negocio.

A continuación vamos a describir las actividades relacionadas con el BIA:

- Analizar el impacto en el negocio (BIA) sobre los servicios críticos que son afectados por los sistemas de información.
- Determinar mediante entrevista y encuestas, el tiempo de recuperación objetivo (RTO), el punto de recuperación objetivo (MTO) y el tiempo máximo tolerable fuera de servicio (MTD) para los sistemas de información críticos y sus componentes o interdependencias requeridos para ser incorporados en la definición de las estrategias de recuperación.
- Elaboración de la matriz para la evaluación de riesgos ante la probabilidad de ocurrencia de una amenaza o desastre natural a los equipos y los sistemas de información dentro de una organización.
- Analizar las medidas de protección y/o prevención que debemos tener en los centros de cómputo contra las diferentes amenazas.
- Evaluar y revisar las medidas de seguridad física que deben tener los sistemas críticos.

- Evaluación y definición de otras soluciones o sitios alternos para el alojamiento de los sistemas de información críticos.

PROPUESTA (OBJETIVOS Y MOTIVACIÓN)

El Instituto para la Formación y Aprovechamiento de Recursos Humanos (IFARHU) es una institución gubernamental la cual tiene como propósito "*Desarrollar un programa que garantice el adecuado aprovechamiento en la formación técnica y la utilización racional de los recursos humanos de la República como medio de acelerar su desarrollo económico y social*".[2]

Para lograr este objetivo el IFARHU se apoya tanto en la infraestructura tecnológica como de los sistemas de información que se encuentran en el centro de cómputo, los cuales son administrados por la Dirección de Tecnología Informática de la institución.

Uno de los aspectos más importantes que debemos considerar en toda gestión administrativa y operativa de un centro de cómputo de una organización es la necesidad de contar con planes de continuidad de las operaciones en caso de que ocurra algún desastre natural o cualquier otro factor, tanto internos como externos que pueda interrumpir los servicios que brindan. Lo anterior nos obliga al desarrollo de una guía o plan de recuperación ante desastres, que ayude a mitigar los riesgos productos de desastres naturales en Panamá y que puedan afectar los servicios que brindan a través de los equipos y sistemas críticos del centro de cómputo del IFARHU.

Por lo tanto, el objetivo general de este trabajo consiste en:

> Elaborar una guía que facilite desarrollar el proyecto de implementación de un DRP para el IFARHU, permitiendo a la Dirección de Tecnología Informática su ejecución dentro de la institución con el fin de contar con plan de acción para

[2] Página web: http://www.ifarhu.gob.pa/ifaweb/Historia3.aspx

mitigar prevenir y/o minimizar el tiempo de la interrupcion por daños y el impacto en el negocio asociado a los procesos criticos de los servicios brindados por TI frente a una contingencia o desastre

Los objetivos especificos de este trabajo son los siguientes

Definir y establecer las etapas o fases requeridas para el desarrollo del proyecto

Realizar un Análisis de Impacto al Negocio para identificar los servicios criticos que brinda el IFARHU

Identificar los posibles riesgos y amenazas naturales que afecta a nuestro pais y a los centros de computo

Analizar las diferentes alternativas de sitios alternos de respaldo asi como los tipos de tecnologias para la replicacion de datos

CAPÍTULO I. ANTECEDENTES.

1.1. ORIGEN DEL IFARHU.

Para los años 60, el gobierno de la República de Panamá para salir delante de la situación económica de esa época, propone la creación de una institución *"que fuera capaz de enfrentar la problemática del recurso humano, proporcionándole al país la mano de obra necesaria para contribuir al crecimiento económico"*.[3] Esto se logra a través de la "Ley No. 1 de 11 de Enero de 1965" y se crea el Instituto para la Formación y Aprovechamiento de Recursos Humanos (IFARHU).

A continuación se describe los cuatro criterios en que se fundamentaron:

1. *"Económico: Para hacerle frente al subdesarrollo, había que educar a un hombre nuevo, con una nueva mentalidad, que contribuyera con una nueva formación y capacitación a impulsar todos los sectores que integran la economía.*
2. *Educativo: Sirviera para disminuir la deserción escolar, por falta de recursos económicos.*
3. *Social: Era difícil impulsar proyectos de crecimiento económico que no fueran correlacionados con la formación y capacitación del Capital Humano.*
4. *Político: Era una necesidad impostergable desprenderse de la dependencia extranjera".*[4]

Para esa época tenían la filosofía que *"para que exista un equilibrado desarrollo económico y social, debe agregarse a las inversiones de orden material y con la debida*

[3] Síntesis de la Evolución Histórica del IFARHU-1989, página 1.
[4] Manual de Organización y Funciones, IFARHU; año 2008, página 1.

- Creación del programa de Perfeccionamiento a Servidores Públicos y Asistencia Educativa.
- Incremento en los montos de los préstamos del Crédito Educativo
- Promueven los estudios y/o investigaciones para determinar las *"...necesidades de formación profesional y técnica..."*.[7]
- Se crea el Departamento de Aprovechamiento de Recursos Humanos, para dar *"...mayor contenido a la filosofía humanística institucional, ya que permite llevar hasta la bolsa de trabajo a los ex- beneficiarios..."*.[8]
- Creación del Centro de Documentación, Información y Orientación Educativa, mediante "Resolución No.820, de 20 de Noviembre de 1979".

En la década de los 80, el IFARHU se caracterizó por "... Incrementar la Asistencia y el Crédito Educativo en todos los rincones de la geografía nacional y convertirlos en una poderosa herramienta de promoción social y económica...".[9]

Nace el lema "EDUCAR PARA EL DESARROLLO" y los programas que se manejaba en esa época fueron: "Crédito y Asistencia Educativa, Planificación de Recursos Humanos, Finanzas, Administración, Información y Documentación".[10]

También se caracterizó que los préstamos y becas se destinaban en su mayoría a *"La juventud humilde y talentosa del país"*.[11]

Se crean los siguientes centros estudiantiles:

- Centro Estudiantil de Coclesito, provincia de Coclé.

---

[7] Memoria 1979, IFARHU, página v.
[8] Memoria 1979, IFARHU, página v.
[9] Memoria 1981, IFARHU, página i.
[10] Memoria 1984, IFARHU, página 9.
[11] Memoria 1984, IFARHU, página 10.

- Centro Estudiantil de La Palma, provincia de Darién.
- Centro Estudiantil de Veraguas.

En la década de los 90, se inicia con una crisis económica que obliga a la administración a realizar una evaluación de todas las Direcciones y Departamentos, incluyendo a las Regionales para determinar su situación real. Se caracterizó por:

- Ampliación y fortalecimiento de los programas tradicionales de becas, crédito y asistencia educativo.
- Creación del programa de *"Asistencia Económica Educativa para los Hijos de los Mártires caídos el 20 de diciembre de 1989"*.[12]
- Creación del programa de Becas para los Corregimientos de Mayor Pobreza.
- Creación del programa de Becas para Estudiantes Discapacitados.
- Promoción de acuerdos y compromisos internacionales.
- Fortalecimiento del Juzgado Ejecutor para la recuperación de la cartera morosa.

Para el año 1996, el IFATHU enfoca sus esfuerzos en *"lograr eficiencia y eficacia de los servicios que se brindan"* [13], para lograr este objetivo trata de impulsar la modernización de la institución a través de la plataforma de tecnología informática, mejorar e incrementar los servicios brindados a través de la especialización de los programas básicos, y mejorar tanto en la eficiencia financiera como administrativa.

Para la década de los años 2000, se caracterizó por:

- Impulsan el fortalecimiento y desarrollo institucional.

---

[12] Manual de Organización y Funciones, IFARHU; año 2008, página 4.
[13] Memoria 1996, IFARHU.

- Implementación en tecnología de informática mediante el equipamiento a nivel nacional para brindar un mejor servicio.
- Disminución del porcentaje del Seguro Educativo para la institución, mediante la "Ley No.49 de 18 de septiembre"
- Creación del programa de Asistencia Educativa *"Nueva Vida"*.[14]
- Incremento del número de becas para los estudiantes.
- Modificación de los reglamentos de becas y préstamos.
- Mejoras en la red de comunicación entre la sede principal y sus regionales.
- Creación de subprogramas como *"Bellas Artes, Formación y Capacitación del Talento Humano en Áreas Prioritarias, Asistencia Económica para la Erradicación del Trabajo Infantil, Pasantías para la Capacitación de Profesionales Agropecuarios en Cultivos de Agro-exportación, Auxilio Económico Complementario, Servidores Públicos y Docentes-Universidades Oficiales, Estudiantes de Escasos Recursos en el Exterior, Pago de Matrícula para Estudiantes de Universidades Oficiales"*.[15]
- Creación del programa de *"Becas Doctorales y Postdoctorales y el Programa de Excelencia Profesional"*.[16]
- Modificación del *"Reglamento de Becas, Asistencia Económica y Auxilios Económicos, reformando la Ley Orgánica No. 1 de 11 de enero de 1965 mediante*

[14] Manual de Organización y Funciones, IFARHU; año 2008, página 5.
[15] Manual de Organización y Funciones, IFARHU; año 2008, página 5.
[16] Manual de Organización y Funciones, IFARHU; año 2008, página 6.

Ley No. 23 de 29 junio 2006, para apoyar la formación del capital humano de acuerdo a lo establecido el Objetivo, Misión y Visión del IFARHU".[17]

- Creación de nuevas formas de créditos educativos a través de la aprobación de un Reglamento de Crédito nuevo, mediante "Resolución No.12 de 28 de diciembre de 2006".
- Aprobación de la *"moratoria y condonación de deuda, beneficiando trece mil ochocientos sesenta y cinco (13,865) prestatarios".*[18]
- Creación de la Oficina de Cooperación Técnica Internacional, por medio de la "Resolución No.320-2006-369 de 28 de julio".
- Creación de las *"Direcciones Provinciales de Ngöbe Bugle y de Emberá en Darién, mediante Resolución No.320-2006-371 de 31 de julio".*[19]
- Mediante "Resolución No. 320-2007-25 de 12 de enero," modifican el nombre de la *"Oficina de la Mujer y pasa a llamarse Oficina de Igualdad de Oportunidades".*[20]
- Creación de la Dirección de Tecnología Informática, mediante "Resolución No. 320-2007-665 de 26 de noviembre de 2007".[21]

Con la modernización del IFARHU, hay que resaltar que nos ha permitido "concretar alianzas con instituciones nacionales y extranjeras, permitiendo la firma de convenios de

---

[17] Manual de Organización y Funciones, IFARHU; año 2008, página 6.
[18] Manual de Organización y Funciones, IFARHU; año 2008, página 6.
[19] Manual de Organización y Funciones, IFARHU; año 2008, página 6.
[20] Manual de Organización y Funciones, IFARHU; año 2008, página 6.
[21] Manual de Organización y Funciones, IFARHU; año 2008, página 6.

cooperación educativa y técnica, prestación de servicios, capacitación de becas y ofertas de crédito".[22]

[22] Manual de Organización y Funciones, IFARHU; año 2008, página 6.

1.2. MISIÓN Y VISIÓN DEL IFARHU.

A continuación presentamos la misión y visión del IFARHU:

1.2.1. MISIÓN.

"Planificar la formación y aprovechamiento del capital humano, otorgar becas a estudiantes destacados, brindar asistencia económica educativa a la población en situación de vulnerabilidad y riesgo, establecer alianzas con organismos e instituciones educativas nacionales e internacionales para darles mayores oportunidades académicas a estudiantes y profesionales talentosos, ofrecer crédito educativo para financiar estudios de grado, postgrado y educación continua en áreas demandadas para el desarrollo integral del país".[23]

1.2.2. VISIÓN.

"Ser la institución líder que oriente, estimule y apoye la formación del capital humano nacional, conforme las áreas demandadas para el desarrollo integral del país". [24]

---

[23] Ver página web: http://www.ifarhu.gob.pa/ifaweb/misionvision.aspx
[24] Ver página web: http://www.ifarhu.gob.pa/ifaweb/misionvision.aspx

1.2. MISIÓN Y VISIÓN DEL IFARHU.

A continuación presentamos la misión y visión del IFARHU:

1.2.1. MISIÓN.

"Planificar la formación y aprovechamiento del capital humano, otorgar becas a estudiantes destacados, brindar asistencia económica educativa a la población en situación de vulnerabilidad y riesgo, establecer alianzas con organismos e instituciones educativas nacionales e internacionales para darles mayores oportunidades académicas a estudiantes y profesionales talentosos, ofrecer crédito educativo para financiar estudios de grado, postgrado y educación continua en áreas demandadas para el desarrollo integral del país".[23]

1.2.2. VISIÓN.

"Ser la institución líder que oriente, estimule y apoye la formación del capital humano nacional, conforme las áreas demandadas para el desarrollo integral del país". [24]

---

[23] Ver página web: http://www.ifarhu.gob.pa/ifaweb/misionvision.aspx
[24] Ver página web: http://www.ifarhu.gob.pa/ifaweb/misionvision.aspx

1.3. OBJETIVOS DEL IFARHU.

Objetivos Estratégicos de la Institución:

- *"Planificar la formación y aprovechamiento del capital humano requerido para el desarrollo integral del país.*
- *Estimular a estudiantes y profesionales panameños de alto desempeño académico.*
- *Apoyar el desarrollo del talento nacional en las artes, el deporte y la cultura.*
- *Administrar efectivamente los recursos para las becas y auxilios educativos provenientes del Estado, personas naturales, entidades públicas y privadas en el nivel nacional e internacional.*
- *Manejar con equidad los fondos destinados por el Estado a la asistencia económica educativa a estudiantes que procedan de la población vulnerable y en situación de riesgo.*
- *Ofrecer crédito educativo para estudios de educación primaria, premedia, media y superior en las áreas demandadas para el desarrollo nacional.*
- *Desarrollar adecuadas políticas y estrategias de cobro que conduzcan a una recuperación eficiente y eficaz.*
- *Modernizar la institución mediante una simplificación administrativa expedita para ofrecer servicios eficientes y eficaces a los usuarios y clientes".*[25]

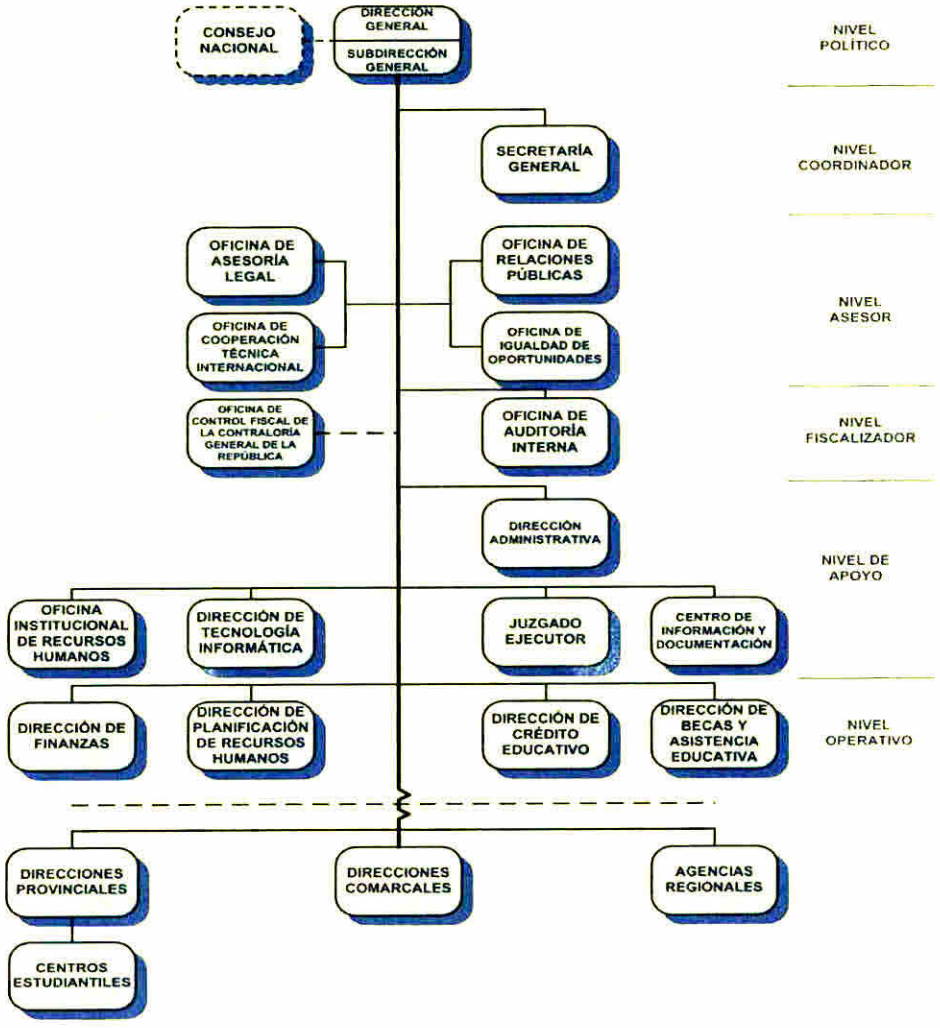
[25] Ver página web: http://www.ifarhu.gob.pa/ifaweb/misionvision.aspx

1.4. ORGANIZACIÓN DEL IFARHU.

El Instituto para la Formación y Aprovechamiento de Recursos Humanos (IFARHU) cuenta con una estructura orgánica bien definida. La misma está compuesta de niveles, además en cada uno de estos niveles se encuentran las áreas o direcciones que conforman cada nivel.

1.4.1. ORGANIGRAMA GENERAL.

Figura 1. Organigrama General del IFARHU. [26]

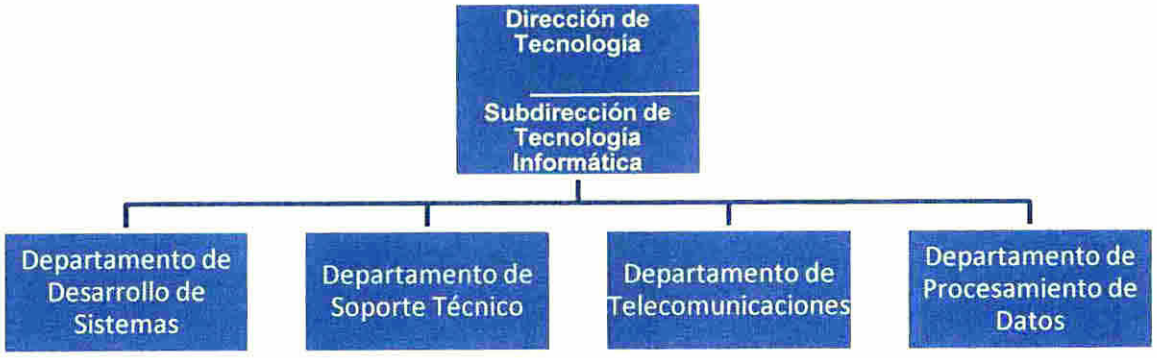


Como se observa en la Figura 1, el IFARHU cuenta con un organigrama bien definido en niveles y estos niveles compuestos por direcciones, áreas y oficinas que apoyan la gestión que la institución realiza. Estas divisiones bien marcadas en el organigrama facilitarán el desarrollo y aplicación del plan de recuperación de desastres.

[26] Ver página web: http://www.ifarhu.gob.pa/ifaweb/Organigrama.aspx

1.4.2 DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA.

Figura 2. Organigrama de la Dirección de Tecnología Informática. [27]



A continuación se describe los objetivos de cada área o sección que compone la Dirección de Tecnología Informática del IFARHU:

- **Dirección de Tecnología Informática:** Su objetivo es *"Planificar, dirigir, organizar, coordinar y supervisar la automatización de los procesos, adquisición y mantenimiento de las tecnologías de información y comunicaciones utilizadas por el Instituto para la Formación y Aprovechamiento de Recursos Humanos a nivel nacional, en apoyo a las directrices emanadas del Despacho Superior y garantizando altos estándares de seguridad en su funcionamiento".* [28]
- **Subdirección de Tecnología Informática:** Tiene como objetivo *"Colaborar con la Dirección de Tecnología de Información y Comunicación en la gestión de los*

[27] Manual de Organización y Funciones, IFARHU; año 2008, página 38.
[28] Manual de Organización y Funciones, IFARHU; año 2008, página 39.

procesos de automatización, adquisición y mantenimiento de las tecnologías de información y comunicaciones utilizadas por el Instituto para la Formación y Aprovechamiento de Recursos Humanos a nivel nacional".[29]

- **Departamento de Desarrollo de Sistemas:** Su objetivo es *"Diseñar, implementar y administrar los Sistemas de Información Tecnológica utilizados por el Instituto para la Formación y Aprovechamiento de Recursos Humanos y todas sus dependencias a nivel nacional, en apoyo a las directrices emanadas de la Dirección de Tecnología Informática".*[30]
- **Departamento de Soporte Técnico:** Su objetivo es *"Diseñar y supervisar los programas de mantenimiento preventivo y correctivo de los equipos computacionales y periféricos que hacen posible el funcionamiento de los Sistemas de Información Tecnológica utilizados por el Instituto para la Formación y Aprovechamiento de Recursos Humanos y todas sus dependencias a nivel nacional".*[31]
- **Departamento de Telecomunicaciones:** Tiene como objetivo *"Diseñar, implementar y administrar de los Sistemas de Telecomunicaciones de Voz, Imágenes, Internet y Datos que hacen posible el funcionamiento de los Sistemas de Información Tecnológica utilizados por el Instituto para la Formación y Aprovechamiento de Recursos Humanos y todas sus dependencias a nivel nacional".*[32]

---

[29] Manual de Organización y Funciones, IFARHU; año 2008, página 41.
[30] Manual de Organización y Funciones, IFARHU; año 2008, página 43.
[31] Manual de Organización y Funciones, IFARHU; año 2008, página 44.
[32] Manual de Organización y Funciones, IFARHU; año 2008, página 45.

- **Departamento de Procesamiento de Datos:** Tiene como objetivo *"Diseñar, implementar, administrar el mantenimiento de la base de datos en los Sistemas de Información Tecnológica utilizados por el Instituto para la Formación y Aprovechamiento de Recursos Humanos y todas sus Dependencias a nivel nacional, en apoyo a las directrices emanadas de la Dirección de Tecnología Informática".*[33]

En cuanto a las funciones de cada sección o departamento están claramente descritos en el Manual de Organización y Funciones del IFARHU.[34]

[33] Manual de Organización y Funciones, IFARHU; año 2008, página 46.
[34] Manual de Organización y Funciones, IFARHU; año 2008, página 39.

1.5. SITUACIÓN ACTUAL.

El IFARHU es una institución gubernamental, orientada a la formación del recurso humano especializado mediante el otorgamiento de becas y créditos educativos para estudios. Para cumplir con las metas y objetivos establecidos de una manera eficaz y eficiente en sus operaciones, se apoya en sus sistemas de información e infraestructura tecnológica.[35]

Actualmente en Panamá, toda gestión relacionada con tecnología en las instituciones gubernamentales es supervisada por la AIG (Autoridad Nacional Para Innovación Gubernamental), quien es la entidad responsable de la modernización del estado panameño, mediante el uso de las Tecnologías de Información y Comunicaciones (TIC's).[36] Todo proyecto o adquisición de hardware y software de las instituciones gubernamentales deben contar con la aprobación la AIG, parte de sus funciones está asesorar y orientarnos en la formulación de nuevos proyectos tecnológicos.

---

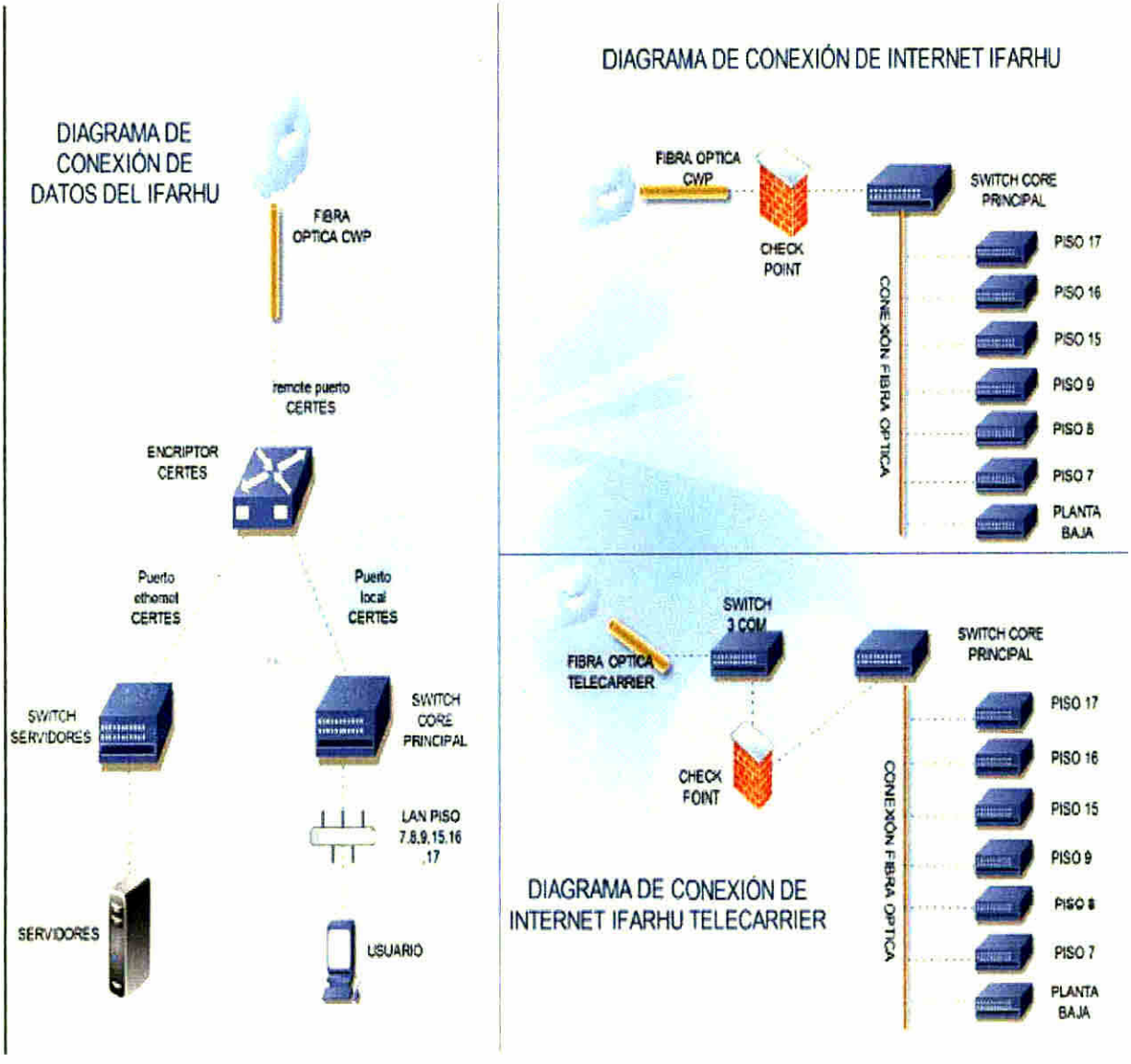
[35] Ver página web: http://www.ifarhu.gob.pa/ifaweb/index.aspx
[36] Ver página web: http://www.innovacion.gob.pa/acercade

1.5.1. CONFIGURACIONES Y TOPOLOGÍAS.

El IFARHU para poder brindar un buen soporte y servicio a los usuarios de nuestros sistemas, debe estar a la vanguardia de los avances tecnológicos y contar con una topología de red adecuada al igual que los equipos configurados correctamente. Cuando mencionamos de topología nos referimos a la forma o estructura como se transmiten los datos en la red, existen tres tipos de topologías básicos: bus, estrella y anillo. En la topología bus, cada computadora se conecta con el servidor a través de un cable central. En una topología anillo, el cableado va de una computadora a otra sin que haya un principio ni un final. En una topología de estrella, todas las computadoras están conectadas al servidor.

La red de área local (LAN) del IFARHU cuenta con una topología tipo estrella, donde los switches de los diferentes pisos del edificio están conectados a través de una fibra óptica hacia el Switch Core principal. En la Figura 3, encontrarán los diagramas de conexión de los datos internos y conexiones de internet del IFARHU.

Figura 3. Diagramas de conexiones de la red del IFARHU.



CAPÍTULO II. METODOLOGÍA.

2.1. CONCEPTUALIZACIÓN DEL DRP.

En esta fase de la metodología, se establecerá las bases conceptuales y el planeamiento inicial para el DRP del IFARHU sobre la cual se desarrolla este trabajo y la coordinación e inducción de los elementos que participan. Este trabajo está enfocado como una guía para la implementación del DRP del IFARHU, sin embargo no podemos entrar en el tema sin tener claro todo los pasos necesarios o requeridos antes de llegar a esta fase. Es por esto que tanto este capítulo como el siguiente (Análisis de Impacto y de Riesgos) guardan relación con otro trabajo como Guía para el desarrollo del DRP para el IFARHU.

Dentro de la conceptualización realizaremos lo siguiente:

- Establecer el alcance del DRP.
- Definir los objetivos.
- Identificar el recurso humano requerido para el desarrollo del DRP de acuerdo a diferentes opciones o alternativas.
- Definir el procedimiento para la aprobación del DRP.
- Desarrollar el procedimiento para la identificación de los desastres probables por amenazas naturales.

2.1.1. ALCANCE.

El alcance de este DRP es que la Dirección de Tecnología Informática del IFARHU cuente con un documento o guía para restablecer las operaciones a nivel de tecnología de la información y por ende de la institución, frente a situaciones o eventos que pudieran interrumpir la continuidad de los servicios brindados afectando así la habilidad de lograr sus objetivos estratégicos, lo cual es un factor clave dentro de cualquier organización.

La utilización y alta dependencia de los equipos tecnológicos y de los sistemas de información ha motivado la necesidad de que la institución debe contar con las medidas preventivas adecuadas, la capacidad y la habilidad para su rápida recuperación, para así seguir brindando los servicios en el tiempo adecuado.

Cuando se desarrollan planes de recuperación de desastres debemos tener en cuenta el alcance del mismo, para lo cual procedemos a definir cuál sería el que utilizaremos en este DRP. Este Plan de Recuperación ante Desastres se desarrollará para los sistemas críticos, cuyas interrupciones sean ocasionadas por fenómenos naturales con la finalidad de mantener la disponibilidad de los servicios críticos que brinda el IFARHU.

2.1.2. OBJETIVOS.

La planeación de un programa de recuperación de desastres es de gran importancia para las instituciones como el IFARHU, ya que al identificar los objetivos del mismo, nos permite desarrollar con eficiencia el contenido del DRP.

Un plan de recuperación de desastres (DRP), puede ser considerado como el plan o guía que ejecutará Tecnología de la Información para recuperar sus sistemas en producción. Por lo tanto el mismo debe contar con un objetivo general y los objetivos específicos. El plan de recuperación frente a desastres, viene siendo aquella parte del plan de contingencia y del plan de continuidad de negocios (BCP), que aborda aquellas contingencias que por su gravedad, no permiten continuar la prestación de los servicios dentro del centro o local actual y debe continuarse el servicio desde un nuevo sitio. El DRP debe contemplar el retorno a la normalidad una vez que hayan solucionado las consecuencias del desastre para que el servicio pueda ser reanudado en el sitio original. Descrito lo anterior procedemos a definir el objetivo general y los objetivos específicos para el DRP del IFARHU.

En la tabla mostrada a continuación, se describen los objetivos generales y específicos que fueron definidos para el desarrollo del DRP del IFARHU.

Tabla 1. Objetivos generales y específicos para el desarrollo del DRP.

TIPO DE OBJETIVO	DESCRIPCION DEL OBJETIVO
General	1. Desarrollar una guía (Plan DRP) que le permita a la Dirección de Tecnología Informática del IFARHU minimizar el tiempo de la interrupción, el daño y el impacto asociado a los procesos críticos del negocio soportados por los servicios brindados por TI, frente al escenario de contingencia.
Específicos	1. Contar con los procedimientos para la recuperación de los sistemas críticos ante desastres naturales, en un lugar alterno y en un tiempo determinado, así como también el procedimiento para devolver los equipos críticos a su centro original cuando termine la contingencia. 2. Dar a conocer a los usuarios claves el contenido del Plan de Recuperación ante Desastres. 3. Establecer políticas para el mantenimiento del Plan de Recuperación ante Desastres.

2.1.3. ALTERNATIVAS PARA EL DESARROLLO DEL DRP.

Para el desarrollo del DRP de los sistemas y equipos que soportan los servicios críticos del IFARHU contemplamos dos alternativas. La primera que sea realizada a través de consultoría externa, y la segunda, que sea desarrollado por el personal de la Dirección de Tecnología Informática (Departamentos de Soporte, Redes y el Director y Subdirector de Tecnología), asesorado por un consultor en Seguridad Informática. Ambas alternativas tienen sus ventajas y desventajas que resumimos a continuación:

Tabla 2. Alternativas para el desarrollo del DRP.

ALTERNATIVAS	VENTAJAS	DESVENTAJAS
CONSULTORES EXTERNOS	- Equipo dedicado para el desarrollo. - Conocimiento especializado en el tema y facilita el desarrollo. - Al ser externos a la institución observan con mayor facilidad nuevos requerimientos. - Generalmente en el desarrollo estos incluyen el mantenimiento del plan.	- Alto costo del desarrollo del DRP. - Dependencia de los consultores externos para actualizar el plan.
PERSONAL INTERNO DE LA DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA Y ASESOR	- Acceso rápido y completo a la información. - Facilidad para realizar el inventario de equipos y su	- Poca experiencia en este tipo de desarrollo. - No es tiempo completo y el proyecto puede durar más

DE SEGURIDAD INFORMATICA	clasificación Conoce todas las medidas de seguridad implementadas Identificar con más facilidad los grupos de trabajo para conformar equipos de DRP No requiere altos costos para el desarrollo del DRP El conocimiento se queda internamente en la institución	tiempo No retención de personal clave para mantenimiento del plan

Luego del analisis en la Tabla 2 se decide realizar el desarrollo del DRP con el personal existente en conjunto con un asesor de Seguridad Informatica y asi disminuir costos para la institucion

2.1.4. ADMINISTRACIÓN DEL DRP.

Para poder realizar la administración del DRP de manera ordenada, se designan responsabilidades específicas y se define el siguiente equipo para su administración:

Figura 4. Diagrama del equipo de administración del DRP

Coordinador de Administración.

Tiene asignado las siguientes responsabilidades:

1. Encargado de supervisar y dar a apoyo al desarrollo de las distintas tareas ejecutadas por los comités que conforman al equipo de administración.
2. Supervisar y colaborar en la ejecución del Plan de Distribución.

Comité de Distribución.

Tiene asignado las siguientes responsabilidades:

1. Garantizar la difusión del plan entre los integrantes del equipo y mantener vigente el Plan de Distribución.

2 Asegurar que los integrantes del equipo de recuperacion ante desastres siempre dispongan como minimo dos copias actualizadas del plan una de las cuales debe mantenerse en el lugar del trabajo y las demas seran almacenadas en algun otro lugar seguro externo al IFARHU

Comite de Entrenamiento

Tiene asignado las siguientes responsabilidades

1 Velar por la definicion y cumplimiento oportuno del Plan de Entrenamiento y Capacitacion de los procedimientos de recuperación

2 Efectuar la planificación de los entrenamientos y notificar a los participantes e instructores acerca de los cronogramas y alcance de las pruebas establecidas

Comité de Pruebas

Tiene asignado las siguientes responsabilidades

1 Supervisar y dar apoyo durante la ejecucion de las pruebas garantizando la ejecucion de las mismas en los tiempos planeados

2 Registrar los resultados de las pruebas y participar activamente en las pruebas

3 Apoyar al personal de las lineas de negocio involucradas en la ejecución de las pruebas

Comite de Mantenimiento

Tiene asignado las siguientes responsabilidades

1 Contar con un conjunto de procedimientos de mantenimiento debidamente formalizados y documentados

2 Revisar y analizar los impactos producidos por cualquiera de los cambios en los ambientes informaticos sobre el Plan de Recuperación de Desastres y proceder a su actualización

3 Debe existir una coordinacion entre el Comité de Distribución y Comité de Pruebas para la actualización de sus respectivos procedimientos de manera que tengan en cuentan los cambios realizados al Plan de Recuperacion de Desastres

2.1.5. APROBACIÓN DEL DRP.

Una vez finalizado el desarrollo del documento denominado Plan de Recuperación de Desastres para los sistemas y equipos críticos que soportan los servicios esenciales del IFARHU, se deberá establecer un procedimiento para la aprobación del mismo. Para que el desarrollo o creación del DRP sea efectiva en instituciones gubernamentales como la nuestra, debemos conformar comités que apoyen la administración del plan y asignarles sus responsabilidades, dentro de las cuales estaría la creación del procedimiento para la aprobación del DRP.

Para esto debemos seguir los siguientes pasos o procedimientos:

1. Un representante de cada Comité en conjunto con Auditoría Interna y el asesor de Seguridad informática deberá evaluar el documento originado por la Dirección de Tecnología Informática.
2. Luego de evaluar el contenido, si todos están de acuerdo se deberá realizar las pruebas al DRP.
3. Una vez realizada estas pruebas y si las mismas son satisfactorias, el Comité de Pruebas en conjunto con Auditoría Interna deberá redactar un informe a la Dirección General del IFARHU indicando la satisfacción del documento denominado Plan de Recuperación de Desastres para los sistemas y equipos críticos.
4. Luego la Dirección General del IFARHU emite un documento donde avala el DRP y solicita a la Dirección de Planificación que incorpore el documento al Manual de Políticas y Procedimientos de la institución.

2.1.6. DESASTRES PROBABLES POR AMENAZAS NATURALES.

Entendemos por amenazas naturales como *"aquellos elementos del medio ambiente que son peligrosos para el hombre, causados por fuerzas extrañas a él"*. Para efectos de desastre, la amenaza *"se refiere a todos los fenómenos atmosféricos, hidrológicos, geológicos (volcánicos y sísmicos), y a los incendios por su ubicación, severidad, y frecuencia que tienen el potencial de afectar adversamente al ser humano, sus estructuras y actividades"*. [37]

A continuación, describiremos las amenazas naturales más comunes agrupadas por categoría física:

Tabla 3. Amenazas naturales más comunes por categoría

Características Físicas	**Amenazas**
Amenazas con características hidrológicas:	1. Inundaciones. 2. Desertificación. 3. Sequía. 4. Erosión y sedimentación. 5. Desbordamientos de ríos. **6.** Inundaciones en edificios causadas por rupturas de tuberías, filtraciones por lluvia.
Amenazas con características atmosféricas:	1. Granizo. 2. Huracanes.

[37] Ver página web: http://www.oas.org/DSD/publications/Unit/oea57s/ch005.htm

	3. Tornados. 4. Tormentas tropicales **5.** Descargas eléctricas causadas por rayos.
Amenazas con características Sísmicos:	1. Fallas geológicas 2. Terremotos 3. Tsunamis
Amenazas con características Volcánicas:	1. Ceniza 2. Gases. 3. Flujo de lava.
Amenazas con características incendios:	1. Matorrales. 2. Bosques. 3. Sabanas. 4. Incendios en edificios.

Según los informes y cronologías de desastres ocurridos en Panamá desde el año 1990 hasta el 2002 [38], ocurren con frecuencia inundaciones y tormentas tropicales que producen descargas eléctricas que afectan equipos tecnológicos. Además para el año 2011 las tormentas tropicales y las inundaciones tuvieron mayor porcentaje de ocurrencia en América, según fuente "Disaster data: A Balanced Perspective", Issue No. 26, Diciembre 2011 [39]. Con lo anterior nos lleva a tomar en cuenta que estas amenazas

[38] Ver página web: http://daraint.org/wp-content/uploads/2012/01/UTR_Panama.pdf
[39] Ver página web: http://reliefweb.int/report/belize/credcrunch-newsletter-issue-no-26-december-2011-disaster-data-balanced-perspective%E2%80%9D

naturales (tormentas tropicales e inundaciones) serían las que pudiesen afectar el centro de cómputo del IFARHU, sin embargo en los capítulos posteriores investigaremos más con el personal de tecnología de la institución y con el SINAPROC (Sistema Nacional de Protección Civil) de Panamá, para obtener sus experiencias y vivencias con los desastres naturales que pueden afectar la ciudad capital de Panamá y por ende el centro de cómputo del IFARHU.

2.2. DISEÑO DEL DRP PARA LOS SISTEMAS CRÍTICOS DEL IFARHU.

Esta sección es fundamental para el desarrollo y posterior implementación del DRP, debido a que realizaremos el inventario de los sistemas de información y los equipos a los cuales se les aplicará el plan de recuperación. Además de identificar este inventario, también vamos a describir más adelante por medio de encuestas donde los directores y jefes de departamentos del IFARHU, identifican los sistemas de información críticos para así poder determinar los equipos críticos donde se encuentran instalados estos sistemas; en este desarrollo del DRP también se tomará en cuenta una de las principales actividades en los centros de cómputo que son los respaldos que realizan periódicamente.

2.2.1. INVENTARIO DE LA PLATAFORMA TECNOLÓGICA.

El inventario de los equipos de la plataforma tecnológica del IFARHU, fue realizado en dos categorías, donde la Tabla 4 muestra o identifica el inventario de servidores y la Tabla 5 muestra los equipos de comunicación.

Tabla 4. Inventario de Servidores del IFARHU.

Inventarios de Equipos del Centro de Cómputo del IFARHU (Servidores y Almacenamiento)						
N°	**MARCA**	**MODELO**	**PROCESADOR**	**DISCO DURO**	**MEMORIA**	**FUNCIÓN**
1	DELL	Modular Chasis PE 1855				Chasis
2	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	No está en uso
3	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	Servidor de Correo Electrónico B2 ***
4	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (RED HAT 4) APLICACIONES B3 ***
5	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (Red Hat 4) Base de datos Oracle B4 ***
6	DELL	POWEREDGE 1855	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	Linux (Vmware esx 3) B5 Servidor de Pruebas (STORAGE 1)
7	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B6 Aplicativo de cajas Bienes patrimoniales
8	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes ***
9	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes *** IfARHU-SIETE, IFARHU-GSI (STOREAGE 1)
10	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) Msa de Ayuda B8 Contenido if-antivirus-01, ifarhu-seis, if-soporte-01, if-sysaid-01, server-printer, servidor printer HP, ssa-if01 (STORAGE 3)
11	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	WS 2008 R2 SERVIDOR DE SEGURIDAD

						(ANTIVIRUS) B9
12	DELL	EMC AX 150		6 X 750 GB		STORAGE 1 (1.5T *** STORAGE 2 (2.0 T) STORAGE 3 (1.0 T)
13	DELL	EMC AX 4-5		12 X 1 TB		PROYECTO IFASIS *** Sistema de Planilla
14	DELL	POWEREDGE 860	INTEL PEMTIUM 2 X 2 (2.8 GHz)	2 X 500 GB	1 GB	WS 2003 R2 (ACTIVE DIRECTORY 1) ***
15	DELL	POWEREDGE 2850	INTEL XEON 2 X(3.40 GHz)	4 X 146 GB	4 GB	WS 2003 SERVIDOR WEB (FEDORA 5)
16	DELL	POWEREDGE 2950	INTEL XEON 4 X (2.0 GHz)	4 X 146 GB	2 GB	WS 2008 R2 servido DHCP ***
17	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 APLICACIONES (WEB)- PROGRAMACION *** Intranet
18	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 BASE DE DATOS (SQL)- PROGRAMACION ***

Tabla 5. Inventario de equipos de comunicaciones del IFARHU.

Inventario de Equipos de Comunicación del IFARHU				
N°	**MARCA**	**MODELO**	**CANTIDAD**	**FUNCIÓN**
1	EXTEME NETWORKS	SUMMIT X460 -24p	3	Switch de piso
2	EXTEME NETWORKS	SUMMIT X460 -48p	2	Switch de piso
3	EXTEME NETWORKS	SUMMIT X450a - 24p	1	Switch de piso
4	CISCO	2800	1	Router
5	3COM	4500	1	Switch
6	MOTOROLLA	RFS 4000	1	Wireless en los pisos
7	CHECK POINT	UTM -1 3070	1	Firewall
8	CERTES	CEP-10 VSE	1	Encripta información entre la Sede y las regionales

2.2.2. EQUIPOS CRÍTICOS DEL IFARHU.

Debido a la importancia de las funciones y operaciones críticas del IFARHU que son apoyadas y soportadas a través der la infraestructura tecnológica descrita anteriormente, se procede a identificar en estos inventarios los equipos que son considerados críticos para la institución. La escogencia es realizada en base a los siguientes criterios:

1. Identificación de los servicios críticos para la institución y los equipos en donde se encuentran instalados.
2. Función que desempeñan estos equipos en el centro de cómputo.

A continuación los servidores y equipos críticos identificados:

Tabla 6. Inventario de equipos críticos del IFARHU.

Inventarios de Equipos Críticos del Centro de Cómputo del IFARHU						
N°	**MARCA**	**MODELO**	**PROCESADOR**	**DISCO DURO**	**MEMORIA**	**FUNCIÓN**
1	DELL	Modular Chasis PE 1855				Chasis
2	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	Servidor de Correo Electrónico B2
3	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (RED HAT 4) APLICACIONES B3
4	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (Red Hat 4) Base de datos Oracle B4
5	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes
6	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes IFARHU-SIETE, IFARHU-GSI (STOREAGE 1)
7	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	WS 2008 R2 SERVIDOR DE SEGURIDAD (ANTIVIRUS) B9
8	DELL	EMC AX 150		6 X 750 GB		STORAGE 1 (1.5 T) STORAGE 2 (2.0 T) STORAGE 3 (1.0 T)
9	DELL	EMC AX 4-5		12 X 1 TB		PROYECTO IFASIS Sistema de Planilla

10	DELL	POWEREDGE 860	INTEL PEMTIUM 2 X 2 (2.8 GHz)	2 X 500 GB	1 GB	WS 2003 R2 (ACTIVE DIRECTORY 1)
11	DELL	POWEREDGE 2950	INTEL XEON 4 X (2.0 GHz)	4 X 146 GB	2 GB	WS 2008 R2 servidor DHCP
12	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 APLICACIONES (WEB)-PROGRAMACION Intranet
13	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 BASE DE DATOS (SQL)-PROGRAMACION

2.2.2.1. CLASIFICACIÓN DE LOS EQUIPOS SEGÚN SU CRITICIDAD.

Luego de identificar los equipos críticos para el centro de cómputo del IFARHU, los clasificaremos según la siguiente escala:

- Sistema crítico alto: Un equipo para el centro de cómputo es considerado como crítico alto cuando una interrupción en uno de ellos, causa la paralización de las operaciones que realiza el IFARHU a través de este equipo y el arreglo o remediación del mismo, puede durar desde uno o varios días. Lo cual trae consigo un alto costo para las operaciones que se efectúan en la institución.
- Sistema crítico medio: Es considerado crítico medio, cuando la interrupción de uno de estos equipos es de manera rápida y el mismo no tiene una gran incidencia en las operaciones que se realicen a través de este equipo. Su recuperación puede durar entre 4 a 8 horas.
- Sistema crítico bajo: Es considerado crítico bajo, cuando su interrupción afecta de manera mínima la operatividad del IFARHU, su recuperación y arreglo puede durar menos de 4 horas.

2.2.2.2. REQUERIMIENTOS NECESARIOS DE LOS SISTEMAS CRÍTICOS.

En esta sección procedemos a identificar los requerimientos en cuanto a software y hardware requeridos para arrancar con el diseño del DRP para la contingencia de los sistemas y equipos críticos:

- Copia de los CD's de instalación de cada uno de los sistemas y equipos críticos.
- Manual, instructivo y procedimiento digital o impreso de la instalación y configuración de cada sistema y equipo crítico.
- CD's de los Sistemas Operativos de cada equipo crítico.
- Respaldo completo de cada uno de los sistemas y equipos críticos.
- Respaldo de los datos de los sistemas críticos, actualizada al último día hábil.
- Manual y procedimiento de restauración de las bases de datos.
- Contratos vigentes de soporte de los sistemas y equipos críticos, con niveles de servicios acordes al grado de criticidad de cada equipo.
- Personal de tecnología y funcional que realizarán las pruebas de los sistemas y equipos cuando se configuren en el sitio alterno.
- Documentación de las pruebas a realizar para los sistemas y equipos.
- Documentación y descripción de los resultados esperados para las pruebas realizadas.

2.2.3. RESPALDO DE LOS SISTEMAS Y EQUIPOS CRÍTICOS.

Una vez identificado los requerimientos necesarios para garantizar la continuidad de las operaciones de los sistemas y equipos críticos o la reducción el tiempo de interrupción de los mismos en caso de ocurrencia de alguna contingencia, pues debemos tener en cuenta otro aspecto importante que son respaldos de los mismos. De manera genérica se requiere resguardar y respaldar:

- Los equipos críticos con características idénticas a los de producción en el sitio alterno.
- Respaldo de las configuraciones (en digital e impresas)
- Manuales de instalación y configuración.
- Procedimientos de instalación y configuración.
- Materiales o la proveeduría necesaria para poder ser utilizados en caso de emergencia (cintas, papel, tóner, cartuchos de tinta, CD's, etc.).
- Un centro de cómputo alterno (secundario) para realizar las mismas operaciones que se efectúan en el primario. Esta instalación debe contener las necesidades básicas para poder realizar el trabajo y brindar el servicio que se brinda en el centro de cómputo primario.
- Una copia del documento Plan de Recuperación ante Desastres del IFARHU en el centro de cómputo alterno para ser utilizado en caso de una contingencia.

Esta es una de las etapas más importantes para el diseño del plan de contingencia, debido a que de nada serviría tener un buen DRP, si no contamos con la información bien ubicado y resguardada para poder ser utilizada ante un case de contingencia.

Además de contar con un personal bien entrenado y que conozca cómo aplicar el DRP en caso de no localizar el personal clave.[40]

[40] Ver página 56 en: http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

2.2.3.1 RESPALDOS Y SU FRECUENCIA.

Para poder definir lo que debemos respaldar y la frecuencia con que debemos realizarlo, se requiere conocer con exactitud la información que vamos a requerir en el caso de que se presenta una contingencia. Es por esto que es de suma importancia tener respaldos de todos los archivos, configuraciones y programas de los sistemas y equipos críticos. Estos respaldos deben incluir:

- Respaldos de software y documentación.
- Respaldos de aplicaciones y documentación.
- Respaldos de bases de datos.
- Respaldos de las configuraciones de los equipos críticos.
- Materiales que sean necesarios para que los usuarios de los sistemas críticos y el personal de cómputo pueda trabajar.
- Copias del DRP.
- Copias de los procedimientos de instalación y proceso de los sistemas críticos.

En cuanto a la frecuencia que se deben realizar los respaldos podemos describir lo siguiente:

- Cuando se adquiera un nuevo paquete de software o se instale una nueva versión de los sistemas operativos de los sistemas críticos. También deben resguardarse una copia de los manuales.
- Cada vez que se actualicen los datos de las bases de datos.
- Cada vez que se modifique algún programa o se instale una nueva aplicación.

- Cada vez que se modifique el DRP se deben proporcionar las copias necesarias para que sean distribuidas al personal clave para la ejecucion del mismo
- Cada vez que se actualice el inventario de equipos criticos se debe guardar la copia mas actualizada
- Cuando se incluya un nuevo material o se modifique los existentes para el procesamiento de los sistemas criticos

2.2.3.2. SITIOS ALTERNOS PARA RECUPERACIÓN.

Debido a los servicios que brinde el IFARHU a los estudiantes y a los ciudadanos, es de vital importancia mantener la continuidad del negocio, esto hace que debemos contemplar la necesidad de tener sitios alternos de respaldo para que en una situación de contingencia podamos continuar las operaciones en ese lugar y seguir brindando el servicio que el centro de cómputo ofrece a sus usuarios.

Este lugar debe tener características muy similares o mejores a las que debe tener actualmente donde se encuentra el centro de cómputo primario. Para nuestro caso existen dos alternativas que deben ser evaluadas, la primera de ellas es tener una empresa que se dedique a realizar este tipo de proceso y que nos proveen los equipos críticos para restaurar el respaldo; y la otra es adquirir o alquilar un local para que el personal de tecnología instale los equipos y sistemas contingentes en este sitio.

Hemos considerado que la primera alternativa es la más factible, debido a que son empresas que se dedican a brindar estos servicios a través su contratación y el nivel de servicio que requerimos, son centros especializados para hospedajes de equipos y sistemas de misión crítica; mientras que la segunda alternativa, además de tener que instalar y configurar los equipos y las aplicaciones, también conlleva a costos de mantenimiento por los aires acondicionados, la electricidad, controles de humedad, controles contra incendios, controles de seguridad de acceso, etc., que tendríamos que implementar y administrar por parte del personal de la institución.

2.3. PROCEDIMIENTO PARA IMPLEMENTACIÓN Y CONTROL DEL DRP.

Posterior al desarrollo del Plan de Recuperación ante Desastres del IFARHU, es necesario que el mismo sea implementado para lo cual debemos llevar a cabo una serie de pasos.

- Hacer un listado de personas a las que se le entregará copias del plan de contingencia (parcial o total).
- Este plan debe contener un directorio telefónico que incluya:
    - Todos los miembros de la Dirección de Tecnología Informática del IFARHU responsables de asistir a implementar el plan en caso de un desastre.
    - El coordinador del plan.
    - Comité de mantenimiento del plan.
    - Comité de pruebas del plan.
    - Auditor de sistemas.
    - Asesor de Seguridad Informática.
- Teléfonos de los responsables del centro de cómputo alterno de respaldo.
- Proveedores de equipos y sistemas críticos.
- Teléfonos de emergencia (Cruz Roja, Bomberos, Policía Nacional).
- Tener una lista de los materiales que se necesitará para la implementación del Plan de Recuperación de Desastres.
- Tener definido y probado los procedimientos para arrancar los sistemas en el sitio alterno.

Después de efectuado los pasos anteriores debemos poner a prueba el DRP para asegurarnos de que el plan tenga los resultados esperados para los cuales fue desarrollado

2.3.1. PUESTA EN MARCHA.

El plan de contingencia debe ponerse en funcionamiento una vez ocurrido el fenómeno natural que afecten a los sistemas y equipos críticos del centro de cómputo del IFARHU. Dentro de las etapas o procesos que debemos considerar para poner en marcha el DRP tenemos:

- El Director o Subdirector de Tecnología Informática del IFARHU deberá informar al equipo administrador del DRP sobre el percance ocurrido.
- El equipo Administrador del DRP en conjunto con personal de Tecnología evaluará los daños.
- El equipo Administrador informará a la alta gerencia sobre el percance.
- Se le solicita la autorización a la alta gerencia para poner en marcha el DRP.
- Se le informa al personal encargado de ejecutar el DRP para que el mismo ponga en ejecución el plan.

2.3.2. PRUEBAS.

Este es un punto importante dentro del Plan de Recuperación ante Desastres debido a que de nada nos sirve tener un plan escrito si el mismo no ha sido sometido a pruebas. Las pruebas al DRP no están incluidas en el alcance de este proyecto, sin embargo describiremos unas consideraciones a tomar en cuenta para cuando se realicen. Al ejecutar las pruebas, se debe identificar aspectos que pueden ser mejorados dentro del plan de contingencia y que a la vez debemos revisar lo siguiente:

- Los procedimientos de recuperación.
- Que existan todos los materiales que se requieran.
- Los respaldos de software, datos y equipos son los adecuados y que los mismos estén actualizados.
- El entrenamiento del personal sea el apropiado.
- El sitio de respaldo externo sea adecuado y cumpla con las necesidades para procesar los sistemas y equipos críticos.

Las pruebas sirven de entrenamiento al personal que ejecutará el DRP cuando esto se requiera. Como propósito primordial las pruebas nos ayudan a identificar posibles deficiencias en los procedimientos que forman parte del plan. Se recomienda hacer una prueba anual del DRP en el sitio alterno de respaldo. Esta nos ayuda a evaluar la eficiencia del plan y a revelar sus carencias para así corregirlas. Existen ciertos requerimientos que se necesitan para la efectividad de las pruebas:

- Se debe establecer el escenario de la prueba.
- Se deben definir los objetivos de la prueba.
- Se deben identificar los resultados esperados en las pruebas.

- Documentar lo anteriormente descrito
- Documentar los resultados
- Hacer partícipe de las pruebas a los auditores para que valide los resultados obtenidos

2.3.3. MANTENIMIENTO.

Todo Plan de Recuperación ante Desastres requiere del mantenimiento continúo, ya que los procesos varían según pasa el tiempo y se anexan nuevos software o equipos que en ocasiones se hacen críticos para la institución. Si el plan no está actualizado, el mismo no podrá ser utilizado de manera efectiva durante un caso de contingencia. Una de las formas de identificar que el DRP requiere ser actualizado, es cuando al mismo se le realizan pruebas.

Al plan de contingencia se le debe dar mantenimiento cada vez que:

- Cambien o aumenten los sistemas o aplicaciones.
- Cambien o se adquieran nuevos equipos.
- Cambie o se actualice el sitio de respaldo externo.
- Cuando se modifiquen los procedimientos y los procesos internos.

Una de las funciones del Comité de Mantenimiento del Plan de Recuperación ante Desastres es revisar que el plan esté actualizado, esto se logra calendarizando las fechas de revisión del DRP. Otro aspecto importante es la distribución de la documentación del DRP, cada vez que se modifica debe distribuirse. De esta manera el Comité de Distribución del DRP mantiene actualizada la última versión del Plan de Recuperación de Desastres de la institución.

CAPÍTULO III. ANÁLISIS DE IMPACTO Y DE RIESGOS.

3.1. ANÁLISIS DE IMPACTO SOBRE EL NEGOCIO.

El Análisis de Impacto sobre el Negocio (BIA)[41] nos ayuda a identificar las áreas cuyas interrupciones en sus servicios pueden afectar de manera significativa el funcionamiento de una organización producto de una contingencia o desastres. En este análisis identificaremos los sistemas y equipos críticos, además estimaremos los tiempos que la institución puede tolerar en caso de un desastre.

Este análisis es considerado como un aspecto primordial en el desarrollo de un DRP, aquí se identifican los diversos eventos que pudieran afectar la continuidad de sistemas y equipos críticos de la institución. En este estudio nos centraremos en identificar dos de las amenazas naturales descritas anteriormente, las más comunes en nuestro país que se han materializado en los últimos 10 años. Además evaluaremos como estos fenómenos puede afectar a los sistemas y equipos críticos de los centros de cómputo.

Según ITIL V3 Fundations dentro de la *"Gestión de la Continuidad de los Servicios de TI"* [42] existe una meta principal y varios objetivos:

- Meta: consiste en soportar el proceso de Gestión de continuidad del Negocio asegurando que tanto los componentes del servicio como los técnicos (computadoras, sistemas, redes, aplicaciones, datos y centros de cómputo) pueden ser recuperados dentro de los tiempos requeridos y acordados con el negocio o institución.

---

[41] Ver página 8 en: http://www.isacamty.org.mx/archivo/213-COBIT_Aplicado_Para_Asegurar_Continuidad_Operaciones.pdf

[42] *Fundamentos de ITIL V3, Cuaderno de Trabajo, Continuidad de Servicio.* [Ontario, Canadá]: 2010. Página 128-141

- Objetivos principales de Continuidad de Servicios de TI segun ITIL V3 Fundations [43]
  - Mantenimiento de los planes para la continuidad de los servicios y los planes de recuperacion de tecnologia de la información que apoya los Planes de Continuidad del Negocio dentro de la organización
  - Llevar a cabo ejercicios de Analisis de Impacto al Negocio (BIA) en forma periodica con lo cual aseguramos que todos estos planes se mantienen alineados con los impactos y requerimientos del negocio los cuales estan en cambios constantes
  - Realizar constantemente la evaluacion y gestión de riesgos para que estos no excedan a los acordados con el negocio y en nuestro caso con la institucion

Para el Analisis de Impacto sobre el Negocio realizaremos una serie de actividades las cuales describimos a continuacion

- Identificación de los sitios físicos Consiste en validar la lista de instalaciones físicas o lugares en donde operan los servicios de TI del IFARHU
- Identificacion de los sistemas de información Se extrae la lista de los sistemas de información que poseen en cada instalacion y se determina cuáles de ellos están interrelacionados de manera directa o indirecta con el servicio de TI
- Evaluacion de la criticidad de los sistemas de información Se clasifica la criticidad de cada uno de los procesos Esta evaluacion es realizada por personal

[43] *Fundamentos de ITIL V3 Cuaderno de Trabajo Continuidad de Servicio* [Ontario Canadá] 2010 Página 128 141

de la institución (Directores y Jefes de Departamento de las areas de servicio de la institucion) Al contar con la evaluación de criticidad de los servicios podemos identificar los sistemas y equipos criticos del centro de computo del IFARHU

- Determinar el RTO RPO y MTD[44] de los sistemas criticos Esto se realizará mediante encuestas o entrevistas al personal clave que maneja la parte operativa de los procesos o servicios que brinda la institucion Una vez conocidos los sistemas de informacion criticos y los equipos criticos del IFARHU encontraremos el tiempo de recuperación objetivo (Recovery Time Objective RTO) el punto de recuperacion objetivo (Recovery Point Objective RPO) y el tiempo maximo tolerable fuera de servicio (Maximun Time Down MTD) para cada sistemas y equipos criticos en el centro de computo del IFARHU para facilitar y ayudar en la definición de las estrategias de recuperación

[44] Ver página web http //seguridadinformacioncolombia blogspot com/2010_05_01_archive html

3.1.1. IDENTIFICACIÓN DE LOS SITIOS FÍSICOS

Actualmente, el IFARHU sólo cuenta con un solo sitio físico o centro de cómputo y se encuentra ubicado en el piso 15 del edificio Unicorp Plaza, ubicado en la Avenida Ramón Arias.

3.1.2. IDENTIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN.

Esta información fue suministrada por la Dirección de Tecnología Informática por medio de entrevista realizada, donde nos indica los sistemas de información que se encuentran alojados en el centro de cómputo de la institución. A continuación se muestra y se identifican los sistemas de información del IFARHU indicados por la Dirección de Tecnología.

Tabla 7. Sistemas de información utilizados en el IFARHU.

Nombre del Sistema	Descripción
Sistema de Crédito	Solicitudes, trámites, desembolso y recuperación de los préstamos educativos
Sistema de Correo Electrónico	Sistema de correo interno, además es utilizado para contactar a los prestatarios y becarios.
Sistema de emisión de Planillas y Cheques	Utilizado para la generación de cheques para el pago a los estudiantes.
Sistema de Becas	Otorgamiento, trámites y seguimiento de becas
Sistema de digitalización de expedientes de crédito	Digitalización de expedientes de crédito

3.1.3. EVALUACIÓN DE LA CRITICIDAD DE LOS SISTEMAS DE INFORMACIÓN.

Esta evaluación fue realizada a través de una encuesta y entrevista a cada uno de los funcionarios (Directores y Jefes de Departamento), fueron 15 personas indagadas donde se les presentó los sistemas de información utilizados en el IFARHU y se les solicitó que nos indicara el nivel de criticidad que ellos consideran para cada uno de estos sistemas de información.

Para definir los niveles de criticidad nos basamos en la clasificación mencionada en el capítulo anterior (Crítico Alto, Crítico Medio y Crítico Bajo). Además se le adiciona a esta evaluación la clasificación "No Crítico", en donde su interrupción no afecta la continuidad del servicio y se les explica a cada uno de los entrevistados estos niveles.

Tabla 8. Encuesta para determinar los niveles de criticidad de los sistemas.

Nombre del Sistema de Información	Descripción	Crítico Alto	Crítico Medio	Crítico Bajo	No Crítico
Sistema de Crédito.	Solicitudes, trámites, desembolso y recuperación de los préstamos educativos.	X			
Sistema de emisión de Planillas y Cheques.	Utilizado para la generación de cheques para el pago a los estudiantes.		X		
Sistema de Correo Electrónico.	Sistema de correo interno, además es utilizado para contactar a los prestatarios y becarios.	X			
Sistema de becas.	Otorgamiento, trámites y seguimiento de becas		X		
Sistema de digitalización de expedientes de crédito.	Digitalización de expedientes de crédito.			X	

Luego de terminada estas encuestas se procede a extraer la información de las mismas donde los resultados fueron los siguientes, que mostramos a continuación:

Tabla 9. Compendio de las encuestas de los sistemas de información críticos.

Nombre del Sistema de Información	Descripción	Crítico Alto	Crítico Medio	Crítico Bajo	No Crítico
Sistema de Crédito.	Solicitudes, trámites, desembolso y recuperación de los préstamos educativos.	12	3		
Sistema de emisión de Planillas y Cheques.	Utilizado para la generación de cheques para el pago a los estudiantes.	2	12	1	
Sistema de Correo Electrónico.	Sistema de correo interno, además es utilizado para contactar a los prestatarios y becarios.	10	3	1	1
Sistema de becas.	Otorgamiento, trámites y seguimiento de becas		10	3	2
Sistema de digitalización de expedientes de crédito.	Digitalización de expedientes de crédito		3	9	3

Luego del análisis del compendio de las encuestas mostrado, podemos indicar el orden de mayor a menor escala en criticidad de los sistemas de información del IFARHU, donde 1 representa la mayor criticidad y el 6 es el de menor criticidad:

1. Directorio Activo (Active Directory).
2. Sistema de Crédito.
3. Sistema de Correo electrónico.
4. Sistema de emisión de Planillas y Cheques.
5. Sistema de Becas.
6. Sistema de digitalización de expedientes.

Al disponer del orden de criticidad de los sistemas de información podemos identificar los equipos críticos y el orden de criticidad de estos. Lo anterior es producto de que si tenemos identificados los sistemas críticos, lo podemos buscar en la Tabla 6 de los equipos críticos del IFARHU e identificar los equipos que soportan a estos sistemas, los cuales describimos a continuación:

Tabla 10. Equipos que soportan los sistemas de información críticos.

N°	MARCA	MODELO	PROCESADOR	DISCO DURO	MEMORIA	FUNCIÓN
	DELL	Modular Chasis PE 1855				Chasis
1	DELL	POWEREDGE 860	INTEL PEMTIUM 2 X 2 (2.8 GHz)	2 X 500 GB	1 GB	WS 2003 R2 (ACTIVE DIRECTORY 1)
1	DELL	POWEREDGE 2950	INTEL XEON 4 X (2.0 GHz)	4 X 146 GB	2 GB	WS 2008 R2 servidor DHCP
6	DELL	EMC AX 150		6 X 750 GB		STORAGE 1 (1.5 T) STORAGE 2 (2.0 T) STORAGE 3 (1.0 T)
2	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (RED HAT 4) APLICACIONES B3
2	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (Red HAT 4) Base de datos Oracle B4
3	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	Servidor de Correo Electrónico B2
4	DELL	EMC AX 4-5		12 X 1 TB		PROYECTO IFASIS Sistema de Planilla
5	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 APLICACIONES (WEB)-PROGRAMACION Intranet
5	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 BASE DE DATOS (SQL)-PROGRAMACION
6	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes

6	DELL	POWI REDGE 1955	INTEL XEON 2 X 4 (3 00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes IfARHU SIFTE IFARHU GSI (STOREAGE I)

En la tabla descrita anteriormente podemos observar la numeracion de los equipos que corresponden y que soportan a los sistemas de informacion criticos Se puede observar que existen 3 renglones con el numero 6 los equipos identificados con este numero son los que soportan el sistema de información con criticidad bajo (Sistema de digitalizacion de expedientes) los equipos identificados con el numero 2 son los que soportan el sistema de informacion denominado Sistema de Credito el cual es considerado como uno más critico para la institución luego del Directorio Activo o Active Directory que guarda toda la informacion relacionada a los usuarios y permisos de acceso a los servidores y dominio del IFARHU

3.1.4. DETERMINAR EL RTO, RPO Y MTD DE LOS SISTEMAS CRÍTICOS.

Según el NIST (National Institute of Standards and Technology), el RTO, RPO y MTD son parámetros que se encuentran relacionados con la Recuperación ante Desastres, por lo tanto deben ser considerados para alcanzar el éxito en la implementación de este plan.

El RTO (Recovery Time Objective) no es más que el tiempo objetivo de recuperación, dicho de otra manera, cuánto puede permanecer la institución (IFARHU) sin la ejecución de una actividad, sin utilizar un sistema de producción o información relevante. Generalmente el RTO se asocia con el tiempo máximo de inactividad. Este tiempo es utilizado para definir con que periodicidad deberá realizar los respaldos de la información; también nos ayuda a decidir la infraestructura adecuada para reactivar nuestras operaciones, en un sitio de respaldo alterno con especificaciones parecidas al primario en la institución, o equipos alojados en otro sitio esperando para restaurar la información respaldada, etc. Si en las encuestas que realizamos para determinar este tiempo, hay un RTO cuya mayoría de los encuestados indiquen que el valor es cero, entonces el IFARHU tendría que contar con una sitio alterno redundante y replicación de datos en línea. Ahora, si el resultado arroja que se debe contar con un RTO de 8, 12, 16, 28 o superior pues bastaría sólo restaurar los respaldos en cintas para cualquier sistema de información crítica en particular.

El Punto Objetivo de Recuperación (RPO), representa el punto en el tiempo antes de una interrupción o falla del sistema, para que el negocio se puede recuperar (teniendo la copia de seguridad más reciente de los datos) después de un desastre o interrupción. A diferencia de RTO, el RPO no es considerado como parte de la MTD, sino un factor de la

cantidad de perdida de datos que el sistema de información puede tolerar durante el proceso de recuperacion El RPO nos debe indicar la cantidad de información que puede la institución perder o sea si el IFARHU realiza sus respaldos todos los dias a las 8 00 p m y el sistema sufre un colapso en el siguiente dia como a las 2 00 p m entonces toda las modificaciones que se realizaron desde el ultimo respaldo se perderá dada a que la misma no se encuentra resguardada en los respaldos El RPO frente a esta situacion representara el respaldo de la informacion que se realizo en la noche anterior Si el IFARHU realiza transacciones a través del Internet entonces el RPO debera ser practicamente igual a cero debido a que debe incluir hasta la ultima transaccion que se realizo De esta manera, el RPO nos indica la clase de proteccion requerida de acuerdo a la informacion que se maneja Con esto podemos considerar que tanto el RTO como el RPO influyen completamente en la alternativa de infraestructura que debemos a considerar para la institucion

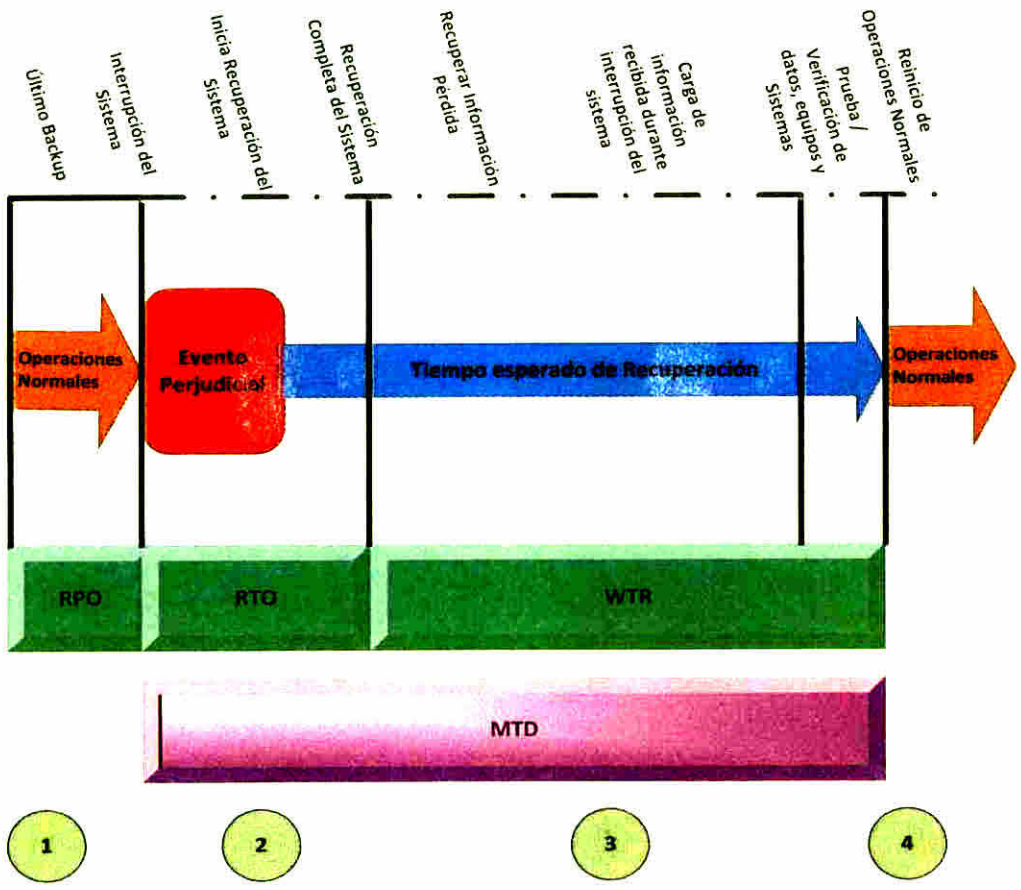
EL MTD (Maximum Tolerable Downtime) se puede definir como el tiempo maximo de inactividad que una empresa u organizacion en ausencia de un proceso puede seguir brindando sus productos o servicios Dentro de una organización es probable que diferentes tareas o procesos tengan diferente tiempo maximo de inactividad Podemos considerar que un MTD es corto cuando un proceso o funcion se encuentra categorizada con prioridad uno Con esto podemos decir que existe una relación entre los procesos criticos de una organizacion y el tiempo maximo de inactividad mientras mas critico sea un proceso menor es el tiempo de espera para poder reiniciar la operacion de este

Si tenemos un tiempo objetivo de recuperacion (RTO) de 8 horas y un tiempo de trabajo en recuperacion (Work Recovery Time WRT) de 16 horas esto significa que

nuestro tiempo máximo de inactividad (MTD) es de 24 horas para un proceso. Por lo tanto, podemos considerar que: MTD = RTO + WRT.

En la siguiente figura podemos observar cómo interactúan estos tiempos, esta información ha sido obtenida del artículo: Análisis de Impacto del Negocio publicado en el 30 de Mayo de 2010 por Leonardo Camelo.

Figura 5. Tiempos RPO, RTO, WRT y MTD del BIA.



Podemos observar el RPO marcado en el punto 1 donde vamos a tener el último respaldo de información realizado y la cantidad de transacciones realizadas hasta que ocurre el evento o incidente que interrumpe la continuidad del negocio. Luego entra el RTO en el punto 2, que abarca desde el momento que ocurre el evento y ponemos en

marcha la recuperación de nuestros sistemas críticos hasta su completa recuperación para operar nuevamente. Después podemos observar en el punto 3 que abarca el WRT, donde restauramos la información del último respaldo realizado en el RPO e iniciamos el proceso para registrar toda la información o transacciones realizadas desde el último respaldo hasta la interrupción del servicio. Posterior a esto, se deben realizar las pruebas y verificación de los equipos, los sistemas y la información que se encuentren todo en orden y al día, para el reinicio de las operaciones normales que se puede apreciar en el punto 4. Se puede apreciar que el tiempo máximo de inactividad (MTD) de la organización comprenderá del tiempo del RTO más el tiempo que dura el WRT hasta que se recupera por completo todos los sistemas para la continuidad del negocio.

El formulario para la encuesta que se utilizó en el IFARHU para obtener los diferentes tiempos que forman parte del BIA lo describimos a continuación:

Tabla 11. Formulario y resultados sobre los tiempos del BIA para los sistemas.

Sistema de Información	RPO (Horas)	RTO (Horas)	WRT (Horas)	MTD (Horas)
Sistema de Crédito	8	7	5	12
Sistema de Correo electrónico	12	8	8	16
Sistema de emisión de Planillas y cheques	16	16	8	24
Sistema de becas	21	16	14	30
Sistema de digitalización de expedientes	28	18	16	34

Esta información lo obtenemos a través de encuestas a los diferentes jefes de departamentos que operan y administran estos sistemas. En la tabla anterior se observa el

resumen y compendio de la encuesta realizada. Teniendo identificado los sistemas de información críticos y sus tiempos de impacto sobre el negocio, podemos identificar el análisis de impacto para los equipos críticos sobre los cuales se encuentran como apoyo o instalado estos sistemas de información. Este análisis de tiempos para los equipos lo realizamos por medio de encuestas a los encargados del departamento de Soporte Técnico y Dirección de Tecnología Informática, basándonos en los resultados de la encuesta para los sistemas de información críticos del IFARHU. Como pueden observar en la tabla siguiente, el MTD se reduce para los equipos dado a que estos debes estar operativos antes de realizar las pruebas de funcionamiento en el sitio alterno donde se encuentran instalados estos equipos. Los números del 1 al 6 indicados en la tabla hacen referencia a los equipos que soportan estos sistemas de la Tabla 10.

Tabla 12. Formulario y resultados sobre los tiempos del BIA para los equipos.

Equipos	RPO (Horas)	RTO (Horas)	WRT (Horas)	MTD (Horas)
1. Equipos para el Directorio Activo y DHCP	4	2	2	4
2. Equipos que soportan el Sistema de Crédito	8	4	4	8
3. Equipos Sistema de Correo electrónico	12	6	6	12
4. Equipos Sistema de emisión de Planillas y cheques	16	10	6	16
5. Equipos Sistema de becas	21	12	8	20
6. Equipos Sistema de digitalización de expedientes	28	14	10	24

3.2 IDENTIFICACIÓN DE POSIBLES RIESGOS Y AMENAZAS NATURALES.

Según el P09 de Cobit (Evaluar y Administrar los Riesgos de TI) nos indica que *"para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados".*[45]

Los riesgos que amenazan el centro de cómputo del IFARHU y los sistemas de información que se ejecuta en la institución fueron identificados por personal técnico de los diferentes de la Dirección de Tecnología Informática del IFARHU y se clasifican en dos grupos: externos e internos.

[45] Ver página 12 en: http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf it.aspx

3.2.1 RIESGOS EXTERNOS.

Son todos los riesgos aquellos que se presentan en el ambiente y que rodea a la instalación del centro de cómputo del IFARHU, por ejemplo:

- Inundaciones.
- Movimientos sísmicos (temblores).
- Tornados.
- Tormentas tropicales.
- Sabotaje.
- Motines sociales.
- Robo (externo).
- Fallas de energía eléctrica.
- Huracanes.
- Maremotos.
- Ataques de virus informáticos.
- Fuego en alrededores del centro de cómputo.
- Daño en los enlaces de comunicación.
- Cierre o paralización de las compañías proveedoras de servicios.
- Cierre o paralización de las compañías proveedoras de suministros de cómputo.

De los riesgos externos que pueden convertirse en las amenazas más comunes en Panamá y que pueden afectar los servicios que se ofrecen a través del centro de cómputo del IFARHU, tenemos los siguientes:

- Tormentas tropicales.

- Inundaciones
- Fallas en la energia electrica

3.2.2 RIESGOS INTERNOS.

Son aquellos que se generan dentro de las instalaciones del IFARHU y en el centro de cómputo, por ejemplo:

- Daños en los equipos.
- Fuego interno (Centro de Cómputo o instalaciones que afecten el área o equipos tecnológicos).
- Equivocaciones de los usuarios del centro de cómputo, provocando daño a equipos, programas, archivos, datos, etc.
- Equivocaciones del personal del centro de cómputo, provocando daño a equipos, programas, archivos, etc.
- Alteraciones o fallas en la energía eléctrica interna.
- Inundaciones internas.
- Falta de aire acondicionado.
- Daño en los UPS.
- Virus informáticos traídos en memorias USB de sus casas o fuentes externas.
- Acceso a información no autorizada.
- Robo de datos por funcionarios o personal de informática.
- Robo interno común, llevándose equipos y/o archivos.
- Fallas en el cableado estructurado.
- Fallas en el software de aplicación. (Office, Sistemas Operativos).
- Fallas en los equipos.
- Falta de actualización de software de aplicación.

- Falta de actualizacion de equipos

De los riesgos internos que pudiesen convertirse en amenazas más comunes para el centro de cómputo del IFARHU y que puedan afectar los servicios que ofrecen tenemos los siguientes

- Inundaciones internas
- Alteraciones o fallas en la energia electrica interna

3.2.3 PONDERACIÓN DEL RIESGO.

Consiste en establecer una calificación en diferentes niveles, para la probabilidad de ocurrencia así como su impacto y poder establecer el nivel de vulnerabilidad del centro de cómputo del IFARHU ante estas situaciones. Durante el proceso de identificación debemos tener en cuenta los factores de riesgo mencionados:

- **Probabilidad de ocurrencia**: Determinar la probabilidad de ocurrencia considerando los controles que se utilizan actualmente y la efectividad de los mismos, así como la frecuencia en la que se puede materializar estos riesgos.
- **Impacto:** Evaluar las consecuencias para el caso en que se materializa el riesgo.

Una vez identificada la ponderación de los riesgos se deben establecer mecanismos para su manejo; existen diferentes maneras o formas para su manejo las cuales describimos a continuación:

- Evitarlo: Modificando los procesos o actividades que generan los riesgos.
- Reducirlo: Aplicando controles para reducir la probabilidad o el impacto.
- Transferirlo: Trasladarlo a otra sección o área de la institución, o adquirir los seguros correspondientes contra estos riesgos.
- Compartir o diversificarlo: Consiste en distribuirlo.
- Asumirlo: Aceptar el riesgo dado que el costo / beneficio de aplicar los controles son mayores a que se produzca el riesgo.

3.2.4 MATRIZ DE RIESGO.

En la siguiente matriz, se describen los riesgos que pueden afectar los sistemas y equipos, y que puede afectar los servicios que ofrece el centro de cómputo del IFARHU a sus usuarios. La misma ha sido desarrollada en base a la identificación de riesgos descrita en el punto anterior, donde cada elemento que compone la matriz nos permite determinar la probabilidad del factor de riesgo que puede ocurrir. Además, se le incorpora también la probabilidad de ocurrencia de los desastres naturales a la matriz de riesgos. A continuación se establece una categorización para los factores de riesgos como de la probabilidad de ocurrencia de los riesgos identificados que puede suceder en las instalaciones del centro de cómputo del IFARHU y son los siguientes:

- Factor de riesgo Bajo. Probabilidad de ocurrencia de 0 a 1.
- Factor de riesgo Medio. Probabilidad de ocurrencia de 2 a 3.
- Factor de riesgo Alto. Probabilidad de ocurrencia mayor a 3.

Tabla 13. Matriz de Riesgos Externos y la probabilidad de ocurrencia.

Descripción del Riesgo Externo	Factor de Riesgo	Probabilidad de Ocurrencia
Inundaciones.	**Medio**	**3**
Desertificación.	**Bajo**	**0**
Sequía.	**Bajo**	**1**
Erosión y sedimentación.	**Bajo**	**0**
Desbordamientos de ríos.	**Alto**	**4**
Granizo.	**Bajo**	**0**
Huracanes.	**Bajo**	**1**
Tornados.	**Medio**	**3**

Tormentas tropicales.	**Alto**	**4**
Descargas eléctricas causadas por rayos.	**Alto**	**4**
Fallas geológicas.	**Bajo**	**1**
Terremotos.	**Bajo**	**1**
Tsunamis.	**Bajo**	**0**
Erupciones volcánicas.	**Bajo**	**0**
Incendios en matorrales.	**Medio**	**2**
Incendios en sabanas.	**Medio**	**2**
Motines sociales.	**Bajo**	**1**
Robo externo.	**Medio**	**2**
Ataques de virus informáticos.	**Alto**	**4**
Fuego en los alrededores del centro de cómputo.	**Medio**	**2**
Daños en los enlaces de comunicación.	**Medio**	**2**
Cierre o paralización de las compañías proveedoras de servicios.	**Medio**	**2**
Cierre o paralización de compañías proveedoras de materiales de cómputo.	**Medio**	**3**

Tabla 14. Matriz de Riesgos Internos y la probabilidad de ocurrencia.

Descripción del Riesgo Interno	**Factor de Riesgo**	**Probabilidad de Ocurrencia**
Inundaciones en edificios causadas por rupturas de tuberías, filtraciones por lluvia.	**Alto**	**5**
Daños en los equipos.	**Medio**	**3**
Fuego interno (Centro de Cómputo o instalaciones que afecten el área o equipos tecnológicos).	**Bajo**	**0**

Equivocaciones de los usuarios del centro de cómputo, provocando daño a equipos, programas, archivos, datos, etc.	**Medio**	**2**
Equivocaciones del personal del centro de cómputo, provocando daño a equipos, programas, archivos, etc.	**Bajo**	**1**
Alteraciones o fallas en la energía eléctrica interna.	**Alta**	**4**
Inundaciones internas.	**Alta**	**4**
Falta de aire acondicionado.	**Medio**	**2**
Daños en los UPS.	**Medio**	**3**
Virus informáticos traídos en memorias USB de sus casas o fuentes externas.	**Medio**	**2**
Acceso a información no autorizada.	**Bajo**	**0**
Robo de datos por funcionarios o personal de informática.	**Bajo**	**0**
Robo interno común, llevándose equipos y/o archivos.	**Bajo**	**1**
Fallas en el cableado estructurado..	**Bajo**	**1**
Fallas en el software de Aplicación. (Office, Sistemas Operativos).	**Bajo**	**1**
Falta de actualización de software de aplicación.	**Medio**	**2**
Falta de actualización de equipos de cómputo.	**Medio**	**2**

En las tablas anteriores el factor de riesgo es clasificado en bajo, medio y alto. Esta referencia es producto de consultas realizadas al personal del departamento de Soporte y Telecomunicaciones del centro de cómputo del IFARHU, donde se les encuestó sobre la incidencia de estos riesgos internos y externos ocurridos en los últimos 10 años. Se

establece que un factor de riesgo es bajo cuando la ocurrencia del riesgo nunca se ha materializado en este lapso de tiempo un factor de riesgo es medio cuando se ha materializado en este lapso de una a tres veces y un factor de riesgo es alto cuando su incidencia haya ocurrido mas de tres veces en este periodo de tiempo

De las dos matrices de riesgos presentadas en las tablas anteriores las dos amenazas naturales que pueden afectar la continuidad de los servicios ofrecidos en el centro de cómputo del IFARHU son los siguientes

- Tormentas tropicales
- Inundaciones internas

Las tormentas tropicales pueden afectar al centro de computo debido a que producto de la gran cantidad de precipitación de agua y vientos producidos pueden afectar el normal funcionamiento de nuestros enlaces y equipos de comunicacion Actualmente en el centro de cómputo del IFARHU poseen ventanas que pueden afectar los equipos y sistemas instalados debido a la entrada o filtraciones de agua vientos y humedad por posibles roturas de las mismas ventanas Otras consecuencias que producen estas tormentas tropicales son las descargas electricas (rayos) y que pueden afectar el suministro electrico y paralizar el funcionamiento del centro de computo por más de 10 horas hasta que se restablece el sistema electrico

3.2.5 PROBABILIDAD DE OCURRENCIA DE LOS DESASTRES NATURALES.

Los desastres naturales son alteraciones ocasionadas por eventos o fenómenos naturales provocando enormes pérdidas materiales y vidas humanas, que superan el límite normal establecido y por lo general se determina a través de algún parámetro o escala. Algunos desastres naturales pueden ser ocasionados por las actividades humanas, tal como la explotación descontrolada de los recursos naturales renovables y no renovables, construcción de viviendas y edificaciones en zonas de alto riesgo, etc.

En la Tabla 13 se describe una lista de posibles desastres naturales y las probabilidades de que estos ocurran en nuestro país y que pueden afectar el centro de cómputo del IFARHU. Esta determinación fue realizada en consenso por los jefes de departamento de la Dirección de Tecnología Informática del IFARHU. Para determinar la probabilidad de ocurrencia, se basaron en las veces que han ocurrido estos fenómenos en nuestro país durante los últimos 10 años y que han podido interrumpir o afectar el servicio de cómputo del IFARHU o de otras instituciones gubernamentales en Panamá. La misma tiene un rango de probabilidad de ocurrencia de 0 a 5, donde 0 es el rango más bajo y 5 el más alto.

Como se observa en la tabla 14, se describen las probabilidades de ocurrencia de los riesgos internos, aunque muchos de estos no son causados por desastres naturales, pero pueden afectar el funcionamiento del centro de cómputo del IFARHU. De lo anterior podemos observar que las inundaciones en edificios producidas por lluvias, tormentas tropicales, descargas eléctricas e incendios en edificios son las comunes en nuestro país.

3.3. PROTECCIÓN DE LOS CENTROS DE CÓMPUTO.

Debido a que el desarrollo del DRP para el IFARHU está enmarcado hacia amenazas naturales, el centro de cómputo donde se albergan estos equipos debe contar con niveles de seguridad física para asegurar la capacidad de supervivencia de la institución ante fenómenos naturales que pueda poner en riesgos el centro de cómputo y por ende los servicios de los sistemas de información que presta la institución. En relación a la seguridad física del Centro de cómputo del IFARHU, esta debe contar con los mecanismos para proteger y conservar los activos (equipos y sistemas) alojados en la misma, en contra de los desastres naturales y de los riesgos que puedan ocurrir, ya sea por actos involuntarios y/o mal intencionados. Debemos asegurarnos que existan los controles adecuados para monitorear las condiciones ambientales, con la finalidad de minimizar los riesgos por fallas o mal funcionamiento de los sistemas, los equipos, las aplicaciones, las bases de datos y de los medios de almacenamiento.

El DRP del IFARHU debe contar con medidas de seguridad ambientales que ayuden a mitigar o reducir los riesgos que puede ocurrir producto de estos fenómenos naturales, estas medidas se describen a continuación:

- Incendios: Estos son causados por el inadecuado uso de materiales combustibles en el centro de cómputo o en sus alrededores y por fallas debido a instalaciones eléctricas defectuosas. Para evitarlos se debe tener el área libre de material combustible e instalaciones eléctricas certificadas por personal idóneo.
- Inundaciones: Se refiere a la invasión de agua o derramamiento de la misma en el centro de cómputo. Lo anterior puede ser producto de que el centro de cómputo se encuentra aledañas a áreas para baños, inodoros, tuberías de aguas negras y

tuberias de agua potable que pasan cerca y que por cualquier desperfecto en estas instalaciones se produce el derramamiento de agua Tambien se puede producir inundaciones debido a las tormentas tropicales y lluvias en donde el area no cuenta con las instalaciones adecuadas y puede producir estos derramamientos dentro del centro de computo esta es una de las causas mayores de desastres en los centros de cómputo Para evitar inundaciones debemos tomar en cuenta lo antes mencionado y evitar instalaciones de centro de cómputo cercano a estas areas de riesgos tambien debe quedar establecido como parte de las politicas de la Direccion de Tecnologia Informatica estas consideraciones al momento de definir las areas para la instalacion de un centro de cómputo alterno

- Humedad Debemos contar con un sensores de temperatura y humedad que puede monitorear el centro de cómputo y que detecte los cambios que puede afectar el normal funcionamiento de los equipos alojados en esta area enviandonos alertas cuando se produce alguna alteracion fuera del rango de los niveles normales y aceptables
- Temperatura El centro de cómputo del IFARHU cuenta con un sistema de aires acondicionados que dan soporte al área donde se encuentran los equipos Además cuenta con aires de contingencia en caso de que el aire principal sufra un desperfecto
- Energia Electrica En Panama las fallas más comunes debido al suministro de energia electrica son las variaciones en el voltaje y la interrupcion en el suministro eléctrico Debido a que cualquiera de estos factores impacta en la continuidad de las operaciones el IFARHU cuenta con

- Utilizacion de UPS con reguladores de voltajes
- Equipo de suministro de energia alterno (Planta Eléctrica)

3.4. SITIO ALTERNO PARA RECUPERACIÓN ANTE DESASTRES.

Es primordial para una institución como el IFARHU contar con un sitio alterno de trabajo, debido a que generalmente los DRP lo establece como requerimiento para poder ejecutar o llevar a cabo la recuperación los sistemas y equipos. Un sitio alterno es una localidad o área de trabajo lo suficientemente distante del original para no ser afectado por el mismo desastre que impacte el sitio principal.

En Panamá existen dos modalidades de sitios alternos según su uso o aplicación, uno para equipos de cómputos y otro para funciones de oficinas. El primero debe contar con todas las condiciones de clima, temperatura, energía eléctrica, sistemas de comunicación y de seguridad que tiene el sitio original; los equipos de cómputos requeridos y la capacidad de las comunicaciones será establecido de acuerdo a lo que se determina en el Análisis de Impacto sobre el Negocio, en relación al mínimo de recursos funcional necesario para apoyar las aplicaciones y equipos críticos. El segundo corresponde a las áreas de trabajo del personal operativo de la institución, el cual no está dentro del alcance de este DRP, ya que sólo está dirigido para los sistemas y equipos críticos de la institución.

La razón principal de un sitio alterno, es para continuar brindando los servicios que el IFARHU presta a sus usuarios y que los inconvenientes que se presenta producto de un desastre no ocasione una paralización completa de las actividades por un largo periodo de tiempo. En la actualidad, el IFARHU no cuenta con un sitio alterno donde colocar sus equipos y sistemas razón por la cual debe incluido en el desarrollo del DRP.

CAPÍTULO IV. IMPLEMENTACIÓN DEL DRP PARA EL IFARHU ANTE AMENAZAS NATURALES.

4.1 DEFINICIÓN DEL PROYECTO.

La intención de este guía es servir como referencia para la implementación de un Plan de Recuperación ante Desastres (DRP) orientado hacia el IFARHU en la Dirección de Tecnología Informática, para esto debemos definirlo como un proyecto. Debido a la alta dependencia de las TIC's en todas las áreas de nuestra institución, es importante contar con la participación de otras Direcciones como Planificación, Finanzas, Administración, Becas y Créditos durante las reuniones iniciales como equipo de trabajo para la definición, elaboración y comunicación sobre este proyecto, pero el principal responsable sigue siendo la Dirección de Tecnología Informática.

Como el DRP está orientado en la recuperación de los sistemas de información y demás componentes de hardware y software dentro la institución, debemos tomar en cuenta tres principios fundamentales al momento de su definición:

- Integridad: Consiste en la protección de todos los datos, su exactitud y confiabilidad, al igual que los métodos de procesamiento.
- Confidencialidad: Es necesario que la información se encuentre accesible sólo a las personas autorizadas.
- Disponibilidad: Consiste en que sólo los usuarios autorizados tengan los niveles de accesos adecuado a la información y a los recursos cuando son requeridos.

Durante esta etapa inicial en las reuniones, se debe revisar y definir lo siguiente:

- Objetivos del proyecto.

- Alcance
- Organizacion de las comisiones y equipos de trabajo
- Mecanismos de comunicacion control y seguimiento
- Plan de trabajo
- Entregables
- Requerimientos
- Criterios de aceptación

Este documento que se genera debe ser revisado y aprobado por la Dirección General del IFARHU para que se le preste la debida importancia al proceso y contar con la cooperacion de todas las áreas involucradas mediante instrucciones giradas por notas Tambien para contar no solamente con el recurso humano requerido sino también con los recursos economicos y destinar los fondos o presupuesto necesario para la implementación del DRP Hay que resaltar que la implementacion de un DRP involucra como parte de los requerimientos contar con sitios alternos de respaldo para mantener la continuidad del negocio Existen diferentes modalidades tipos de sitios alternos que dependerán de la estrategia o mecanismos que adoptemos como solucion asi mismo serán los costos

4.2 REVISIÓN DE LAS POLÍTICAS Y ORGANIZACIÓN.

Esta es una de las actividades que debemos realizar en conjunto con la Dirección de Planificación para la implementación del DRP. Consiste en la revisión de las políticas establecidas en el Plan de Continuidad en el Negocio (BCP) y sus componentes, tales como la identificación de los requerimientos, normas y objetivos estratégicos definidos. Su finalidad es mantener y garantizar el funcionamiento claramente establecido por el negocio frente a cualquier evento de desastre, interrupción o contingencia.

Los planes, disposiciones y medidas establecidos en el BCP garantizan la supervivencia de una organización, al asegurar la entrega de los productos o servicios críticos que brinda una organización, evitando cualquier problema legal o contractual existente. Dentro del BCP, deben estar claramente identificados todos los recursos necesarios para garantizar la continuidad del negocio, incluyendo personal, información, equipos, recursos financieros, apoyo legal, seguridad y alojamientos en caso de requerirse.

Por su parte el DRP consiste en un plan diseñado para restaurar la operatividad de los sistemas de información, aplicaciones y facilidades de cómputo en un sitio alterno de respaldo después de una contingencia o desastre. La implementación y desarrollo de este plan, puede significar la diferencia entre recuperar los servicios de TI y garantizar la continuidad del negocio en horas y minutos hasta varios días en caso de no estar preparados adecuadamente. Por lo tanto, los objetivos que establecemos en el DRP del IFARHU tienen que estar alineados con lo establecido en el BCP, para que cumpla con su función y logre alcanzar el objetivo deseado.

Adicional a la revision de las politicas del BCP y definicion de los objetivos y alcance del DRP debemos definir la organizacion de la estructura requerida para el desarrollo y la implementación de nuestro DRP Por lo tanto debemos incluir el recurso humano requerido de acuerdo a las alternativas presentadas en Tabla 2 donde se escoge la segunda alternativa y el desarrollo del DRP sera llevado a cabo por personal interno de la Dirección de Tecnologia Informatica y adicional a esto vamos a requerir de un asesor en Seguridad Informática con experiencia que haya participado en la implementación de DRP Se definen las comisiones tanto para la dirección del proyecto como los comités para la ejecucion y desarrollo del DRP con sus responsabilidades ver punto 2 1 4

Toda esta documentación debera ser presentada a la Direccion General para su revisión sustentacion y aprobacion

4.3 ANÁLISIS DE IMPACTO AL NEGOCIO (BIA).

En esta fase tiene como objetivo reconocer, medir y calificar el impacto sobre el negocio debido a la interrupción de las operaciones dentro de nuestra institución. La información recabada en este análisis sirve como base o fundamento para determinar las estrategias de recuperación más adecuada para su implementación que trataremos más adelante.

A través del BIA se identifica los procesos y sistemas críticos, para así estimar el tiempo que la institución puede tolerar en caso de una contingencia o desastre, también nos permite dimensionar las medidas de prevención y recuperación de acuerdo a nuestras necesidades, evitando así los costos de inversión demasiado alto o demasiado bajo.

Entre las tareas que se realiza en esta etapa tenemos:

- Identificación de los procesos.
- Identificación de los servicios ofrecidos y su dependencia de los sistemas de información.
- Definición de los niveles de impacto y criticidad de los sistemas de información.
- Dependencias entre los sistemas de información y su relación con la infraestructura instalada.
- Entrevista y desarrollo de cuestionarios con los usuarios y dependientes de los sistemas de información.
- Estimación de los tiempos máximo tolerable fuera de servicio (MTD), tiempo de recuperación objetivo (RTO) y punto de recuperación objetivo (RPO).

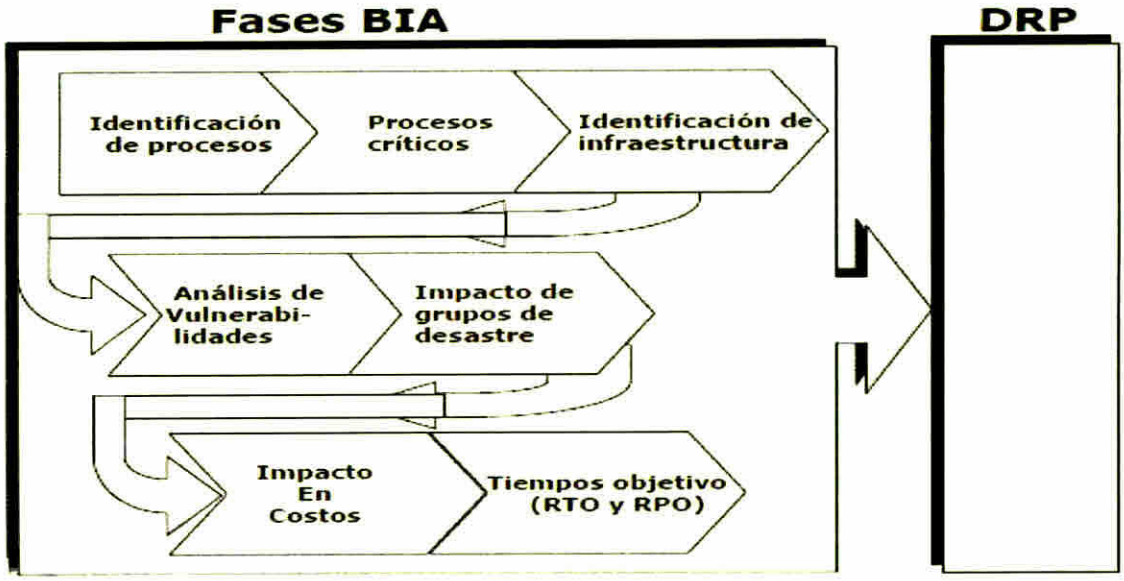
Es importante tener actualizado el inventario de los equipos (Tabla 4) y sistemas de información (Tabla 7) que tenemos en ejecución dentro de nuestra institución, una vez

identificados los sistemas criticos a través de entrevistas realizadas y su ponderacion mediante encuestas podemos establecer su relación con el hardware utilizado tales como servidores cantidad de procesadores memoria discos duros internos o externos sistema operativo etc En la Tabla 4 se encuentra el inventario de los servidores realizado por personal de la Tecnologia y en la Tabla 6 se encuentran los equipos criticos de acuerdo a las aplicaciones los sistemas y las bases de datos que son de vitales para el funcionamiento y continuidad de las operaciones que brinda el IFARHU

Con respecto a esta fase o etapa para la implementacion del DRP ya se tiene en este documento como referencia parte del trabajo realizado con respecto al inventario de los sistemas de informacion y su criticidad de acuerdo a las encuestas realizadas (Tabla 9) asi como los equipos criticos que soportan a estos sistemas de información (Tabla 10) Tambien se identifico en el BIA los tiempos de requeridos RTO RPO WRT y MTD de los sistemas de informacion y equipos criticos identificados en el IFARHU (Tabla 11 y 12)

La documentacion sobre los resultados obtenidos del Analisis de Impacto al Negocio (BIA) debe ser revisada y aprobada por parte de la Dirección General esta etapa es imprescindible para el alineamiento del DRP con los objetivos de la institución A continuación se puede observar las diferentes fases del BIA

Figura 6. Fases del Análisis de Impacto al Negocio (BIA).[46]



[46] Hernández, M. *Implementar DRP en el sector financiero.* México: 2011. Online Disponible en: <http://www.tlalpan.uvmnet.edu/oiid/download/Implementaci%C3%B3n%20DPR_04_PO_PINN_E.pdf>. p. 12.

4.5 ESTRATEGIAS DE RECUPERACIÓN.

Con la información generada del BIA en la etapa anterior, se establece y se seleccionan los métodos de operación alternativos que se utilizarán una vez ocurrido la interrupción y así mantener la continuidad de los procesos y servicios críticos de la institución y sus dependencias, de acuerdo a las prioridades y tiempos establecidos en el BIA.

Entre las actividades a realizar tenemos:

- Revisar el alcance y los hallazgos del BIA.
- Presentar y analizar diferentes opciones de estrategias.
- Debe presentar también el análisis de costo beneficio, análisis FODA y los tiempos de recuperación (RTO) de las estrategias analizadas.
- Revisar y seleccionar las estrategias a seguir, estas deben ser aprobadas por la Dirección General del IFARHU.
- Establecer los proyectos y definir los responsables del desarrollo de planes de recuperación asegurando que las mismas se encuentren alineados a las estrategias seleccionadas.

La escogencia de la estrategia va a depender de los siguientes aspectos:

- Criticidad del proceso a proteger.
- Costo de la estrategia.
- Tiempo de recuperación objetivo (RTO).
- Punto de recuperación objetivo (RPO).
- Nivel de riesgo, dispuesto a enfrentar por la institución.

4.4 EVALUACIÓN DE RIESGOS.

Consiste en identificar y evaluar los riesgos relacionados que pueden afectar la continuidad del negocio, debido a la probabilidad de ocurrencia y el impacto que pueden tener estas amenazas ocasionando interrupciones en los servicios brindados por nuestra institución.

Entre las tareas que debemos realizar son:

- Identificar los riesgos o amenazas internos y externos que pueden afectar la continuidad del negocio.
- Determinar el factor de riesgo a través de ponderaciones y su impacto dentro de nuestra organización.
- Determinar la probabilidad de ocurrencia de los riesgos o amenazas a través de información estadísticas.
- Establecer las prioridades y determinar las medidas adecuadas para el tratamiento de los riesgos identificados, a través de alternativas como evitarlo, reducirlo, transferirlo, diversificarlo o aceptarlo.

En la Tabla 15, se encuentra identificado los diferentes tipos de amenazas, los desastres probables y el grado de ocurrencia de estos fenómenos naturales que sucede en Panamá. De los cuales podemos llegar a la conclusión que las causas principales y más comunes que pueden afectar a los centros de cómputo son las inundaciones producto de las lluvias y tormentas tropicales, al igual que las descargas eléctricas e incendios.

Dentro de las estrategias para la continuidad de los servicios tenemos las medidas preventivas para evitar la interrupcion de los servicios y las medidas reactivas para la recuperación de los servicios en a sus niveles aceptables en el menor tiempo posible
Entre las medidas preventivas tenemos el fortalecimiento y protección perimetral de nuestra infraestructura tecnologica o centro de computo a traves de utilizacion de

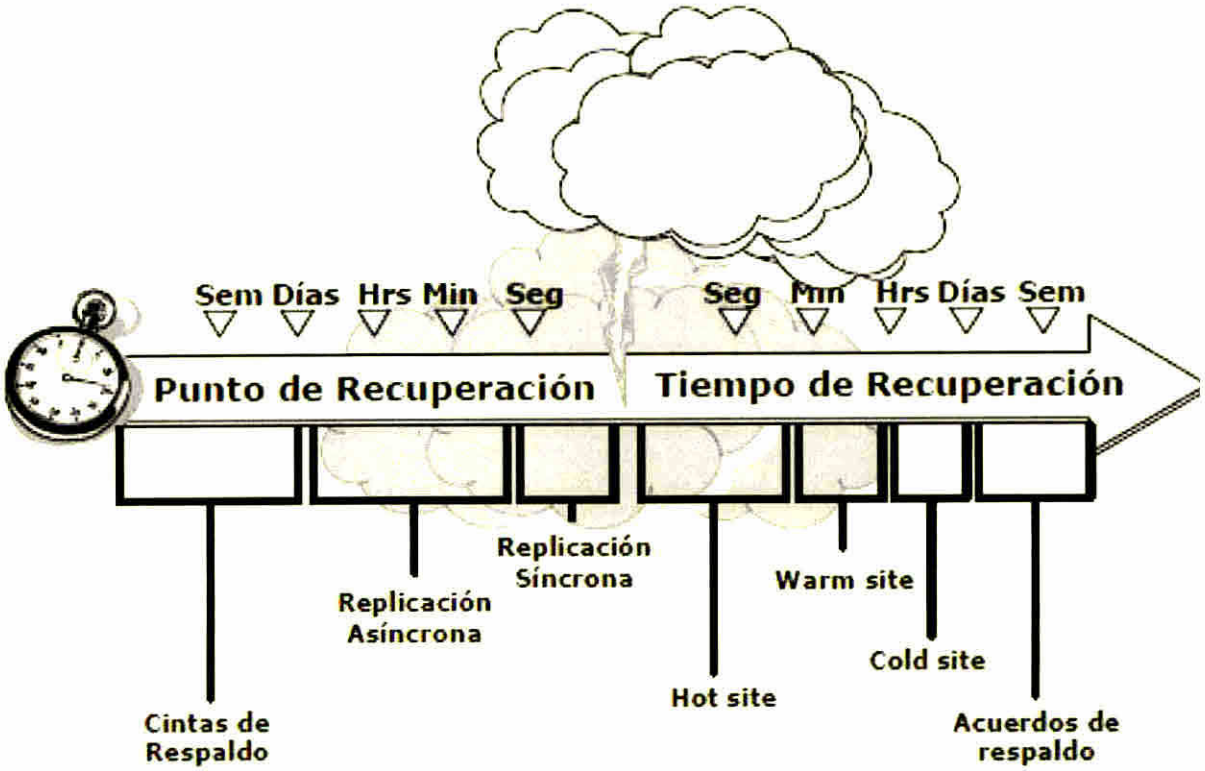
- Sensores ambientales (para determinar temperatura humedad etc)
- Sensores de humo
- Extintores
- Piso falso
- Banco de bateria (UPS) con reguladores de voltajes
- Aire acondicionado de respaldo
- Respaldo de los datos aplicaciones y configuraciones de los sistemas
- Plantas eléctricas
- Controles de acceso etc

Aun con todo lo que implementamos para la estrategia de mitigar o reducir la interrupción de los servicios no estamos exentos que tarde o temprano vamos a encontrar una situacion que no puede ser evitado con las actividades de prevención Esto conlleva a la necesidad de evaluar otras estrategias de continuidad y recuperación del servicio segun las necesidades de nuestra institución

Parte de un DRP se encuentra el establecimiento de un sitio alterno de respaldo en caso de que ocurra alguna contingencia o desastre natural este debe estar situado a una distancia reglamentaria para evitar ser afectada por la misma situación que el sitio

primario. En la siguiente figura podemos observar diferentes estrategias de continuidad en un sitio alterno de respaldo:

Figura 7. Estrategias de Continuidad.[47]



[47] Hernández, M. *Implementar DRP en el sector financiero.* México: 2011. Online Disponible en: <http://www.tlalpan.uvmnet.edu/oiid/download/Implementaci%C3%B3n%20DPR_04_PO_PINN_E.pdf>. p.15.

4.5.1 SITIOS ALTERNOS.

Entre las diferentes alternativas que debemos evaluar y seleccionar referentes a los sitios alternos de respaldo son los siguientes:

- Hot site: Estos sitios están listos para operar en pocas horas, tiene el equipo, la red y los sistemas necesarios. Requiere de una estructura alterna con replicación de datos continuo y que todos los sistemas se encuentren preparados para la sustitución inmediata de la infraestructura de producción. Es la alternativa más costosa y debe ser considerada para el caso en que una interrupción de los servicios de TI tiene grandes repercusiones en nuestra institución.
- Warm site: Estos sitios puede operar en menos de un día, está parcialmente configurado con conexiones de red y equipo periférico seleccionado, tiene una capacidad de CPU menor a la de producción normal. Esto opción requiere de una estructura alterna con sistemas ya activos para la recuperación de los servicios críticos en un período de 24 a 72 horas.
- Cold site: Sólo posee la infraestructura básica, como suministro eléctrico, aire acondicionado, etc. Se encuentra listo para recibir el equipo de cómputo y comunicaciones, esto hace que pueda demorar varios días para iniciar las operaciones. Estos sitios requiere de una estructura donde podemos levantar en pocos días nuestro nuevo sitio de producción. Sería la alternativa más adecuada si se determina que la institución puede seguir operando y brindando sus servicios sin el apoyo de la infraestructura tecnológica.
- Acuerdos recíprocos: Son acuerdos de respaldo entre dos o más organizaciones, para apoyarse mutuamente cuando ocurre una contingencia o emergencia.

Como pueden observar la seleccion de una alternativa debe estar alineada con las politicas establecidas sobre la continuidad de los servicios su criticidad y su impacto en nuestra institución por la interrupción de estos Los costos de inversión van a variar de acuerdo a la alternativa seleccionada y su complejidad Ver Anexo A – Requisitos en el centro de datos alterno esto puede servir como referencia de algunas caracteristicas que debemos contemplar al momento de la contratación del servicio

4.5.2 REPLICACIÓN DE DATOS.

La replicación consiste en una solución a través de software, por medio de la cual mantenemos copias o respaldo de los datos del sistema principal para que pueden ser recuperados en otros sistemas alternos. Es importante contar el respaldo de los datos fuera del sitio primario o en una ubicación remota para mantener la continuidad de las operaciones, la utilización de estos respaldos de datos en los sitios alternos como almacenamiento puede reducir el tiempo de recuperación de nuestros servicios críticos. Entre las opciones o alternativas a considerar con respecto a este punto, tenemos los siguientes:

- Replicación síncrona: Durante este tipo de replicación, los datos no se validan en los discos duros hasta que lo hacen en la ubicación remota. Por lo tanto, es de vital importancia el rendimiento del vínculo de las comunicaciones y de los sistemas de almacenamiento en la ubicación remota. Si la comunicación es lenta, el servidor antepondrá las necesidades de sincronización frente a las peticiones de los usuarios, con la consiguiente reducción del tiempo de respuesta del usuario.
- Replicación asíncrona: Consiste en que cada réplica suele estar desincronizada, no espera la validación en la ubicación remota. Al igual que la opción anterior, si la comunicación es lenta, se le da prioridad a la replicación en lugar del rendimiento de las aplicaciones, por lo que reduce el tiempo de respuesta de los usuarios.
- Cintas de respaldo: Se consideran también como un método de replicación, no es más que simples copias de seguridad realizada en los sistemas de producción que pueden ser restaurada en un sistema alterno.

Como pueden observar el metodo de replicación tiene que ir acompañado del tipo de sitio alterno que seleccionamos y asi mismo implica un grado de inversion en la infraestructura de comunicación lo cual puede conllevar un alto costo si requerimos de la recuperacion de la continuidad de los servicios de TI en el menor tiempo posible

4.5.3 CLÚSTER.

Consiste en un grupo equipos o servidores interconectados a través de una red de alta velocidad, de tal manera que es visualizado como un sólo servidor. Para que un sistema de clúster funcione no es necesario de todos los equipos tengan el mismo hardware y sistema operativo. Para esto requiere de un interfaz de manejo de clústeres que se encarga de interactuar con el usuario y los procesos, repartiendo la carga entre los diferentes equipos. La implementación de este tipo de sistema tiene como finalidad disponer de servicios de:

- Alto rendimiento.
- Alta disponibilidad.
- Equilibro de carga.
- Escalabilidad.

El clúster funciona a través de diferentes componentes, pero debe contar con la certificación para este tipo de esquema. Los componentes que la integran son los siguientes:

- Nodos (servidores o PC de escritorio).
- Sistema operativo (de entorno multiusuario).
- Conexión de red (pueden variar entre simples conexiones Ethernet hasta sistemas de alta velocidad como Gigabit Ethernet, SCSI, etc.).
- Middleware (software que actúa entre el sistema operativo y las aplicaciones, brindando al usuario la experiencia de estar utilizando una única súper máquina).
- Protocolos de comunicación y servicio.

- Aplicaciones

La implementacion de clusteres no solo se limita a un sitio principal sino también que puede estar disperso geograficamente y los datos pueden replicarse a traves de un vinculo WAN Cuando se encuentra disperso geograficamente debe tener ciertas consideraciones como la configuración de una matriz de almacenamiento en cada sitio los nodos del cluster deben estar conectados al subsistema de almacenamiento de tal forma que cuando ocurre un error en un sitio o un error de comunicacion entre sitios los nodos que aun funcionan pueden conectarse al sistema de almacenamiento en su propio sitio

La implementacion de cluster por replicacion de datos puede ser considerada como la mejor alternativa para lograr el requisito de disponibilidad continua facilitando la rapida recuperacion contra las diferentes interrupciones de los servicios y proporcionando una mayor flexibilidad La inversion dependera de los servidores (cantidad y velocidad de CPU tipo de sistema operativo espacio en disco cantidad de memoria) que puede implicar una inversión de nivel intermedio hasta un nivel alto

4.6 DESARROLLO DEL DRP.

Para facilitar el desarrollo del DRP, el IFARHU designará un equipo de administración para el DRP que estará integrada por diferentes comité, cada una con responsabilidades asignadas (ver Figura 4).

El DRP puede definirse como el plan que ejecuta las TIC's para la recuperación de los sistemas gestionados. Por lo general, este consiste en un plan enfocado y diseñado para TI con el propósito de restaurar la operatividad de los sistemas, aplicaciones o facilidades de cómputo en un sitio alterno después de una contingencia o desastre. En esta fase para la implementación del DRP, consiste en desarrollar el plan y los procedimientos de recuperación para las operaciones críticas después de un evento de desastre o contingencia, que haya interrumpido la continuidad de los servicios y por ende a la institución. Estos planes a desarrollar deben estar alineados con las estrategias de recuperación previamente seleccionadas.

En esta etapa, también se desarrolla los planes de restauración y retorno a la normalidad de las operaciones, tan pronto se haya restablecido el sitio primario y sus recursos de operación.

Entre las actividades que se realiza tenemos los siguientes:

- Designar el personal responsable para la elaboración y revisión de las tareas específicas de recuperación.
- Establecer el contenido de los planes, sus componentes, estructura y formato.
- Recopilar la información requerida para contenido de los planes.
- Desarrollo de los planes con su documentación.
- Establecer la logística para la documentación de los planes.

- Distribución de los planes para su revision (mediante el Comite de Distribución establecido por el IFARHU)
- Adecuar los planes y establecer el mecanismo para su aprobación (ver punto 2 1 5)
- Asesoramiento por parte de los responsables en las actividades para el desarrollo de esquemas de operacion alternativos

El desarrollo del DRP debe contemplar siempre la peor de las situaciones de esta manera podemos enfrentar y resolver la contingencia en el menor tiempo posible Mencionamos la importancia de contar con un sitio alterno de respaldo pero seria inutil sin un Plan de Recuperación ante Desastres Esto debe servirnos como una guia que describa paso a paso dentro del proceso de recuperacion incluyendo

- Los eventos que pueden indicar posibles desastres
- Procedimiento de emergencia para asegurar la seguridad del personal incluyendo procedimiento de evacuacion Ver Anexo B – Directorio de servicios de emergencia dependiendo de la gravedad del evento debemos tener a mano los teléfonos de las diferentes autoridades que debemos llamar para nuestro caso en el IFARHU
- Las personas dentro de la institución que tienen la autoridad para declarar un desastre y por ende activar el DRP Ver ejemplo en el Anexo C – Formato de evaluación del desastre nos puede servir para documentar los detalles del evento y la autorización para dar inicio a la ejecucion del DRP
- La identificacion de los procesos de negocio y recursos de tecnologia de la información que deben ser recuperados

- La secuencia de pasos requeridos para preparar el sitio alterno de respaldo una vez que se haya declarado el desastre
- La información de las personas afectadas y los responsables por cada actividad del DRP incluyendo la información de los contactos
- La informacion de los proveedores externos y los contratos de garantia y servicios de los equipos y sistemas criticos Ver Anexo D – Directorio de proveedores externos de equipos esto nos puede servir para contactar al proveedor del equipo o servicio en un caso necesario
- El rol y la responsabilidad del personal clave para la ejecución del plan Un ejemplo sobre este punto lo podemos considerar en el Anexo E – Directorio del equipo de recuperacion ante desastres para el caso nuestro en el IFARHU
- Un inventario del hardware y software necesario para el restablecimiento de las operaciones
- Un listado del personal que cubrira el sitio alterno incluyendo un horario de rotación para soportar las operaciones continuas evitando el desgaste del personal durante la contingencia
- La secuencia de pasos requeridos para mover las operaciones del sitio alterno nuevamente al sitio primario una vez que haya finalizado la contingencia Para esto debemos tomar en cuenta y evaluar las condiciones y el estado de los equipos si operan de manera adecuada o si sufrió algun daño ver Anexo F – Reporte de equipos evaluados
- Los procedimientos de comunicación con empleados autoridades clientes y publico en general

Las actividades que se realizan en un DRP se clasifican de la siguiente forma

- Actividades previas al desastre Son las tareas como la planeacion desarrollo capacitacion y ejecucion de las actividades de respaldo de la información que nos permite asegurar la recuperacion en el menor tiempo posible al menor costo
- Actividades durante el desastre Son aquellas que se realiza una vez presentada la situacion de contingencia o desastre como las actividades contenidas en el plan de recuperacion de los servicios para la continuidad del negocio
- Actividades despues del desastre Son aquellas tareas posteriores al desastre como el plan de restauración del sitio primario

Es importante que los procedimientos establecidos en el DRP sean entendibles por cualquier persona que lo pueda llevar a cabo y que todos los cambios se encuentren actualizados y documentados debido a que ante una situación de emergencia el plan puede ser la unica ayuda que le permita reconstruir y restaurar las operaciones de la institución

4.7 ENTRENAMIENTO DEL PERSONAL.

Consiste en el desarrollo y ejecución de un plan para concientizar y entrenar el personal responsable del DRP para la recuperación y restauración de los sistemas de la institución. Las actividades que se ejecutan son:

- Definir los conocimientos que deberá adquirir el personal involucrado.
- Definir la logística y el personal o audiencia para el adiestramiento.
- Puesta en marcha del plan de entrenamiento.

Dentro de la capacitación inicial, deberá incluir en el temario: las estrategias del DRP y su organización, la estructura y contenido de los planes, las responsabilidades del personal involucrado; así como el apoyo para el mantenimiento y prueba de los planes establecidos.

Existirá el Comité de Entrenamiento para el DRP del IFARHU, que se encargará de velar por la planificación y el cumplimiento del plan de entrenamiento y capacitación de los procedimientos de recuperación, mediante la calendarización de estos eventos y notificando al personal que participará como a los instructores.

4.8 PRUEBAS DEL DRP.

El plan de recuperación de continuidad debe ser probado con el fin de determinar si funciona adecuadamente o si deben ser corregidas y actualizadas partes del plan. En esta etapa se desarrolla el plan de pruebas y los ejercicios para los planes de recuperación teniendo en cuenta diferentes tipos de pruebas. El Comité de Pruebas tendrá la responsabilidad de vigilar que se efectúe las pruebas según lo establecido en la calendarización, también de los resultados obtenidos los cuales se le hará participe a Auditoría Interna para la validación de las mismas.

Los puntos que deberá ser tomado en consideración durante esta etapa son:

- Definir el alcance de las pruebas y sus objetivos.
- Análisis de los costos y aprobación del presupuesto.
- Definir y asignar el personal involucrado.
- Desarrollo de los escenarios y supuestos.
- Evaluar su impacto en producción.
- Dirigir el plan de pruebas y ejercicios.
- Registrar y reportar los resultados obtenidos.
- Realizar las correcciones de los planes según los hallazgos.

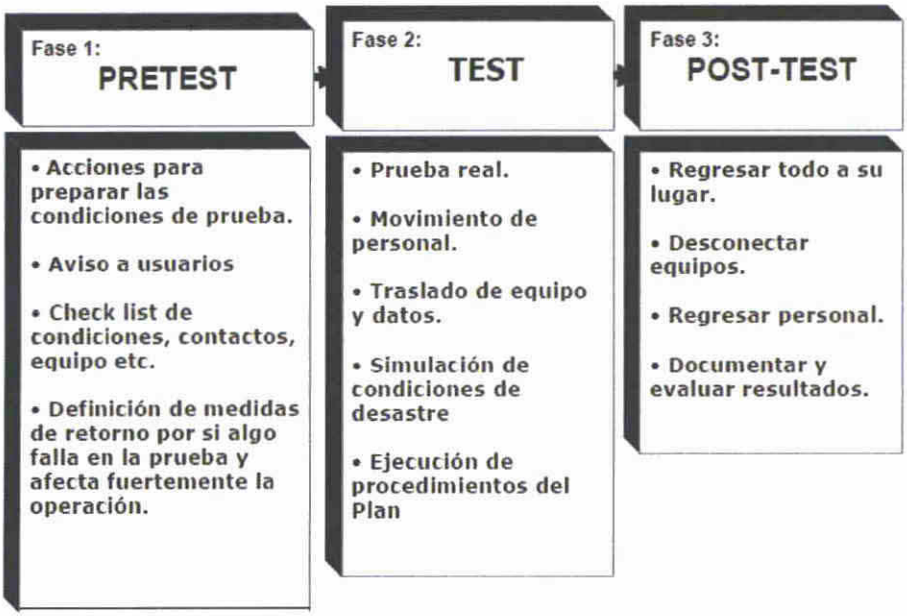
Las pruebas deben ejecutarse durante el tiempo en que se afecte mínimamente las operaciones normales, tal como los fines de semana. Estas pruebas deberán contemplar los elementos críticos y simular las condiciones de proceso lo más parecidas a las normales de operación. Las pruebas deberán incluir lo siguiente:

- Verificar la totalidad y precisión del plan.

- Evaluar el desempeño del personal involucrado.
- Evaluar la coordinación entre las diferentes áreas de la institución.
- Medir la capacidad del sitio alterno para la ejecución del proceso requerido.
- Identificar la capacidad de recuperación de los registros e información vital.
- Evaluar el estado, cantidad de equipos y suministro que han sido trasladado al sitio de recuperación.
- Medir y evaluar el desempeño de los sistemas operativos y computacionales.

A continuación se muestran las fases de uno de los tipos pruebas denominado "Full Interruption Test", la cual es una prueba real que tiene como finalidad detener el sitio primario de producción y trasladar todas las operaciones a las instalaciones y facilidades alternas.

Figura 8. Fases del proceso de Full Interruption Test [COBIT].[48]



[48] Hernández, M. *Implementar DRP en el sector financiero.* México: 2011. Online Disponible en: <http://www.tlalpan.uvmnet.edu/oiid/download/Implementaci%C3%B3n%20DPR_04_PO_PINN_E.pdf>. p.16.

4.9 MANTENIMIENTO DEL DRP.

Consiste en desarrollar un plan para el mantenimiento y actualización del DRP, con el objetivo de asegurar que todas las áreas involucradas están debidamente preparadas para el manejo de cualquier evento o incidente que pueden afectar la continuidad del negocio, sin importar los cambios de diferentes índoles.

Los principales disparadores para el mantenimiento son:

- Revisión periódica del DRP mediante una programación establecida.
- Actualizaciones del plan debido a cambios en los sistemas o infraestructura.
- Modificaciones y mejoras al plan por los resultados obtenidos en las pruebas y ejercicios.

Debido a los cambios constantes en la tecnología de la información, es importante mantener actualizado el plan cada vez que:

- Adquirimos o realizamos cambios en los sistemas.
- Adquirimos nuevos equipos e infraestructura de comunicación.
- Cuando realizan cambios en el sitio alterno de respaldo.
- Cuando se modifican las políticas y procedimientos internos de la institución.

Por esto es importante que el Comité de Mantenimiento del DRP del IFARHU este constantemente revisando el plan y que se encuentre actualizado para que cumpla con su función, para ello se establece fechas de revisiones periódicas. Luego que se actualiza la documentación del DRP, a través del Comité de Distribución se le hará llegar la última versión actualizada del DRP del IFARHU a todo el personal involucrado.

CONCLUSIONES

Actualmente, con los avances de las TIC's junto con los costos accesibles, las empresas u organizaciones tienen una alta dependencia de los sistemas de información y de su infraestructura tecnológica para las diversas operaciones o servicios que brindan. Todos estos centros de procesamiento de datos que hoy en día son Gerencias o Direcciones de Tecnología, han evolucionado y cuentan con un presupuesto de inversión y otro de funcionamiento. Es por esto que ha ido ganando un lugar dentro de la organización y pueden sugerir o decidir lo que es más conveniente sobre esta materia.

Esto nos hace recapacitar sobre lo que debemos hacer y es seguir modelos existentes y estándares establecidos que han demostrado ser eficientes y exitosos. El IFARHU como institución gubernamental no puede quedar rezagado frente a estos constantes cambios, podemos tener claramente definido los objetivos y políticas del Plan de Continuidad del Negocio (BCP) en un documento, pero requiere del apoyo del equipo tecnológico para que se haga realidad. Por lo tanto, es de vital importancia que la Dirección de Tecnología Informática contribuya en hacer cumplir lo establecido en el BCP a través de la implementación de un Plan de Recuperación ante Desastre (DRP) para garantizar la continuidad y disponibilidad de los servicios que brinda nuestra institución.

Esto conlleva a realizar una serie de etapas o fases, donde una de las primeras actividades es alinear el DRP con las políticas establecidos en el BCP, para asegurar que el desarrollo del plan y su implementación cumplan con su función. En la Dirección de Tecnología Informática sólo cuenta con documentación de los diferentes procesos, pero se necesita más que esto para poder tener el producto final deseado que es el DRP.

Otra fase importante para lograr el desarrollo del DRP y que debemos considerar es el Análisis de Impacto del Negocio (BIA), donde se identifica los servicios críticos y sus dependencias, así como los tiempos de recuperación (RTO, RPO y MTD) de los mismos. Los resultados obtenidos del BIA contribuyen y nos ayuda a tener una base para el desarrollo del DRP, permitiendo seleccionar la mejor alternativa y solución que se ajuste a las necesidades del IFARHU y evitando así los sobre costos de inversión.

Por último, una vez desarrollado el DRP del IFARHU es importante que los diferentes comités creados sigan cumpliendo con sus responsabilidades designados para el mantenimiento y actualización, pruebas, entrenamiento y distribución del DRP por los cambios o modificaciones que va sufriendo la institución con los avances tecnológicos y que estos sigan alineados con las políticas establecidas.

RECOMENDACIONES

Entre las recomendaciones que podemos resaltar en este trabajo tenemos los siguientes:

- Presentar y sustentar la importancia de la definición y ejecución del proyecto para la implementación de un Plan de Recuperación ante Desastres (DRP) para el IFARHU.
- Revisar y actualizar los objetivos y políticas establecidas en el Plan de Continuidad del Negocio (BCP) de la institución, para que el DRP a implementar se encuentre alineado con este.
- Involucrar a los directores y jefaturas para la participación activa y cooperación en el análisis y desarrollo del proyecto.
- Revisión del Análisis de Impacto sobre el Negocio (BIA) y de los riesgos identificados en la institución, para su presentación ante la Dirección General, directores y diferentes jefaturas involucrados.
- Establecer la importancia de que el IFARHU tenga un sitio alterno de respaldo para mantener la continuidad del negocio y cumplir con las políticas establecidas.
- Definir y evaluar diferentes alternativas de recuperación para la continuidad del negocio, estudiando modelos implementados con éxito y las tecnologías utilizadas.
- Análisis de costos y beneficios de las alternativas propuestas para su selección e implementación.

- Creación de los grupos de trabajos y comités para la elaboración y desarrollo del DRP de acuerdo a las alternativas seleccionadas.
- Definir un calendario para revisiones periódicas del DRP y así garantizar la actualización y mantenimiento del plan.
- Establecer un plan de prueba, ejercicios y simulaciones periódicamente, para asegurarnos de la calidad y confiabilidad del DRP.
- Establecer un plan de entrenamiento y capacitación calendarizado, para la actualización y concientización del personal involucrado durante la ejecución del DRP ante la declaración de una contingencia o desastre.
- Involucrar al personal de Auditoría Interna de la institución durante las pruebas y también la ejecución del DRP ante una contingencia, para evaluar los resultados obtenidos y aportar recomendaciones.
- Mantener en forma permanente los comités creados para el mantenimiento, pruebas, entrenamiento y distribución de la última versión del DRP.

GLOSARIO DE TÉRMINOS

BIA: Análisis de impacto del negocio. Siglas en inglés: Business Impact Analysis.

BCI: Instituto de Continuidad del Negocio. Siglas en inglés: Business Continuity Institute.

CD: Disco compacto utilizado para almacenar información. Siglas en inglés: Compact Disk.

COBIT: Objetivos de Control para la Información y Tecnologías relacionadas. Siglas en inglés: Control Objectives for Information and related Technology.

DRII: Siglas en inglés: Disaster Recovery Institute International.

DRP: Plan de Recuperación ante Desastres. Siglas en inglés: Disaster Recovery Plan.

Firewall: Sistema de seguridad para redes basado en reglas donde el tráfico de entrada y salida de los paquetes de datos debe pasar por un sistema que puede autorizar o denegar su paso, de acuerdo a las políticas de control de acceso entre redes.

ITIL: Biblioteca de Infraestructura de Tecnologías de Información. Siglas en inglés: Information Technology Infrastructure Library.

MTD: Tiempo máximo tolerable fuera de servicio. Siglas en inglés: Maximun Time Down.

NIST: Instituto Nacional de Estándares y Tecnología. Siglas en inglés: National Institute of Standards and Technology.

P09: Proceso de COBIT - Evaluar y Administrar los riesgos de TI.

Routers: Es un dispositivo utilizado para enrutar paquetes entre redes, además permite interconexión entre estas.

RPO: Punto de recuperación objetivo. Siglas en inglés: Recovery Point Objective.

RTO: Tiempo de recuperación objetivo después de un desastre. Siglas en inglés: Recovery Time Objective.

Scripts: Son conjuntos de instrucciones o comandos que permiten la automatización de tareas.

SAN: Es una red de área de almacenamiento. Siglas en inglés: Storage Area Network.

Switches: Son dispositivos digitales lógicos para la interconexión de redes de computadoras.

USB: Dispositivo de almacenamiento que utiliza una memoria flash para guardar información. Siglas en inglés: Universal Serial Bus.

UPS: Fuente ininterrumpida de poder. Siglas en inglés: Uninterruptible Power Supply.

WRT: Tiempo de trabajo en recuperación. Siglas en inglés: Work Recovery Time.

REFERENCIAS BIBLIOGRÁFICAS

- EC-Council. *Disaster Recovery*, Volume 1 of 2 mapping to ECDR/ECVT Certification. USA: Cengage Learning, 2011.
- Rittinghouse, J.; Ransome J. *Business Continuity and Disaster Recovery for InfoSec Managers*. UK: Elsevier Digital Press, 2005.
- Snedaker, S. *Business Continuity & Disaster Recovery for IT Professionals*. USA: Syngress Publishing, 2007.
- Schmidt, K. *High Availability and Disaster Recovery: Concepts, Design, Implementation.* Germany: Springer, 2006.
- International Information Systems Security Certification Consortium, *Business Continuity and Disaster Recovery Planning, in The Official (ISC) 2 CISSP CBK Review Seminar*, Student Handbook, Version 12.0. Massachusetts, USA: High Stakes Writing, 2011.
- Hiatt, Ch. *A Primer for Disaster Recovery Planning in an IT Environment*. USA: Idea Group Publishing, 2000.
- Bajada, S. *ITIL Foundatios*. GTS Learning Group, 2007.
- P.M.I. (Project Management Institute). *Guía de los Fundamentos de la Dirección de Proyectos, PMBOOK Guide*. (Tercera Edición) USA: 2004.
- Pink Elephant. *Fundamentos de ITIL V3, Cuaderno de Trabajo, Continuidad de Servicio*. Ontario, Canadá: 2010. p. 128-141
- IFARHU. *Manual de Organización y Funciones*. Panamá: Departamento de Desarrollo Institucional, actualización 2012. Online. Disponible en:

<http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf>.

- Rengifo, F., Méndez, N., Méndez, M. Topologías más Comunes. 2007. Online. Disponible en: <http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml>.
- Espinosa, N.; Panadero, E. *La necesidad de implantación de un Plan de Continuidad de Negocio*. Madrid, España: Borrmart, 2005. Online. Disponible en: <http://www.borrmart.es/articulo_redseguridad.php?id=564>.
- Ferrer, R. *Política de Continuidad del Negocio (BCP, DRP)*. Bogotá, Colombia: 2009. Online. Disponible en: <http://www.sisteseg.com/files/Microsoft_Word_-_POL_TICA_DE_CONTINUIDAD_DEL_NEGOCIO.pdf>.
- GCP Global. *DRP y BCP: Continuidad Operativa*. México: 2008. Online. Disponible en web: <http://www.gcpglobal.com/docs/Continuidad_BCP_DRP.pdf>.
- Donoso, Y.; Ferrer, R. *Planes de Recuperación ante Desastres DRP*. Colombia: 2010. Online. Disponible en web: <http://www.acis.org.co/fileadmin/Conferencias/DRP_BCP.pdf>.
- Salazar Villalobos, J. *Guía para crear un Plan de Recuperación en caso de desastre en el sistema informático del centro de datos de un grupo financiero.* San José, Costa Rica: enero 2008. Online. Disponible en: <http://www.uci.ac.cr/Biblioteca/Tesis/PFGMAP505.pdf>.
- Biblioteca Virtual en Salud y Desastres Guatemala. *Registro de desastres Naturales*. Panamá: 2006. Online. Disponible en web: <http://desastres.usac.edu.gt/documentos/pdf/spa/doc16425/doc16425-3b.pdf>.

- I.P.M.D. *Amenazas Naturales*. Panamá. Disponible en web: <http://ipmd.tripod.com/id31.html>.
- Sanahuja, Harris E. *Condiciones y Capacidades para la Reducción del Riesgo, País Piloto: Panamá*. 2011. Online. Disponible en: <http://daraint.org/wp-content/uploads/2012/01/UTR_Panama.pdf>.
- Guha-Sapir, D. *Natural disasters in the American continent*. GredCrunch Newsletter, Issue No. 26, December 2011 – *"Disaster Data: A Balanced Perspective"*. Disponible en web: <http://reliefweb.int/report/belize/credcrunch-newsletter-issue-no-26-december-2011-disaster-data-balanced-perspective%E2%80%9D>.
- IT Governance Institute. *COBIT PO 7.5 Dependencia sobre Individuos*. 2007. Online. Disponible en: <http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf>.
- Peña Ibarra, J. A. *De la Teoría a la práctica: CobiT aplicado para asegurar la continuidad de las operaciones*. México: 2005. Online. Disponible en: <http://www.isacamty.org.mx/archivo/213-COBIT_Aplicado_Para_Asegurar_Continuidad_Operaciones.pdf>. p. 8.
- Camelo, L. *Análisis de Impacto de Negocios / Business Impact Analysis (BIA)*. Bogotá, Colombia: mayo 2010. Online. Disponible en: <http://seguridadinformacioncolombia.blogspot.com/2010_05_01_archive.html>
- Hernández, M. *Implementar DRP en el sector financiero.* México: 2011. Online Disponible en: <http://www.tlalpan.uvmnet.edu/oiid/download/Implementaci%C3%B3n%20DPR_04_PO_PINN_E.pdf>.

- Ven, K.; De Haes, S.; Verelst, J.; Van Grembergen, W. *Using CobiT 4.1 to guide the adoption and implementation of Open Source software*. 2008. Online. Disponible en: <http://www.isaca.org/Journal/Past-Issues/2008/Volume-3/Documents/jpdf0803-using-cobiT-4.1.pdf>.
- Joannis, L. *La importancia de un DRP*. México: Milenio, 2012. Disponible en web: <http://www.milenio.com/cdb/doc/impreso/9163135?quicktabs_1=1>.
- Ferrer, F.; Ferrer R. *Auditoría BCP, DRP*. Colombia: 2009. Online. Disponible en web: <http://www.sisteseg.com/files/Microsoft_PowerPoint_-_Auditoria_Plan_de_Continuidad_BCP_DRP.pdf>.
- British Standards Institution. *Business Continuity Management – Part 1: Code of Practice*. London. UK: BSI, 2006. Online. Disponible en: <http://www.zarifopoulos.com/files/BS-25999%20Business%20Continuity%20Certification_pending.pdf>.
- British Standards Institution. *Business Continuity Management – Part 2: Specification*. London. UK: BSI, 2007. Online. Disponible en: <http://www.govchina.org/Soft/UploadSoft/201204/2012041608115777.pdf>.
- Swanson, M.; Bowen, P.; Wohl Phillips, A.; Gallup, D.; Lynes, D. *Contingency Planning Guide for Federal Information Systems*. NIST Special Publication 800-34 Rev. 1. USA: NIST, mayo 2010. Online. Disponible en: <http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf>.

- Wallace, M.; Webber, L. *The Disaster Recovery Handbook: a step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets*. USA: AMACOM, 2004.
- Gustin, J. *Disaster & Recovery Planning: a guide for facility managers*. (5th Edition) USA: The Fairmont Press, 2010.
- Gregory, P. *IT Disaster Recovery Planning for Dummies*. USA: Wiley Publishing, 2008.
- Maiwald, E.; Sieglein, W. Security Planning & Disaster Recovery. California, USA: McGraw-Hill/Osborne, 2002.

Otros sitios consultados:

- ANAM (Autoridad Nacional del Ambiente). Sitio web: http://www.anam.gob.pa/
- Contraloría General de Panamá. Sitio web: http://www.contraloria.gob.pa/
- ETESA (Empresa de Transmisión Eléctrica, S.A.). Sitio web: http://www.hidromet.com.pa/cuencas.php
- Instituto de Geociencias de la Universidad de Panamá. Sitio web: http://www.igc.up.ac.pa/index.php
- SINAPROC (Sistema Nacional de Protección Civil). Sitio web: http://www.sinaproc.gob.pa/

ANEXOS

ANEXO A - Requisitos en el centro de datos alterno.

Los controles mencionados dependen de lo contratado con el proveedor, en caso que el centro de contingencia sea a través de un tercero. Así mismo se debe revisar periódicamente las condiciones y funcionamiento de los servidores, servicios de contingencia y librerías de backup.

No	Requisito	S/N
	Controles Generales	
1	Detectores de Humo	
2	Sensores de Temperatura	
3	Extinguidores (Tipo A/B/C/D)	
4	FM200	
5	Switch de corte de energia	
6	Detector de aniego	
7	Fuente de alimentación de energía externa	
8	Aire acondicionado (requerimientos mínimos de BTU)	
9	Falso piso / techo	
10	Cableado debidamente etiquetado bajo el falso piso	
11	Rack para servidores (con llave)	
	Monitoreo de Seguridad Física	
1	Cámaras de vigilancia	
2	Controles Biométricos	
3	Sensores de Movimiento	
	Controles para Contingencia	
1	UPS	
2	Planta Eléctrica	

ANEXO B - Directorio de servicios de emergencia.

No.	Empresa	Teléfonos
1	**SISTEMA NACIONAL DE PROTECCIÓN CIVIL (SINAPROC)**	*335
2	**COMPAÑÍA DE BOMBEROS**	
	Central de Emergencias	103
3	**POLICÍA NACIONAL**	104
4	**DEFENSA CIVIL**	
	Central de Emergencias	228-2187 *455
5	**AMBULANCIAS**	
	Alerta Medica	911
	Ambulancia	264-4122
	SEMM	366-0122
	EMI	236-6060
6	**IDAAN**	
	Centro de Atención Ciudadana	311
7	**UNION FENOSA**	
	Contacto	315-7222 800-8346

ANEXO C - Formato de evaluación del desastre.

Descripción del Evento	
Fecha	/ / Hora : am/pm
Notificado por:	_____ <indique el personal que notificó el evento>
Breve descripción del Evento:	<describa brevemente el evento>
Tipo de desastre:	<indique el tipo de desastre: Incendio, Terremoto, Sobre carga / falta de energía, Inundaciones, Huelgas, Falla en los sistemas ambientales, Mal tiempo>
Daño ocasionado:	<describa el daño ocasionado a la infraestructura e instalaciones>
Tiempo requerido para reparación:	<indique el tiempo requerido para completar la reparación> <En caso el tiempo requerido para completar la reparación de los daños sea mayor al tiempo de recuperación requerido por el negocio, se declara la situación de emergencia>
Locación de los puntos de encuentro	
Sitio de Recuperación de TI	<indique el sitio donde se procederá a recuperar el centro de datos>
Declaración del desastre	
Fecha	/ / hora : am/pm
Autorizado por	_____ _____ <colocar los nombres y firmas de las persona que declaran el desastre para proceder a operar en contingencia> _____

ANEXO D - Directorio de proveedores externos de equipos.

Empresa	Servicio	Contacto	Teléfono Fijo	Celular	Dirección
	Servicio de mantenimiento preventivo y correctivo de servidores DELL				
	Servicio de Soporte y Mantenimientos de Equipos de Comunicaciones.				
	Servicio de Mantenimiento del Firewall.				
	Servicio de soporte de comunicaciones.				
	Servicio de unidades de Almacenamiento				
	Servicio de mantenimiento preventivo y correctivo de servidores HP				
	Empresa encargada de Custodia de Cintas de backup				

ANEXO E - Directorio del equipo de recuperación ante desastres.

Función		Rol	Posición	Nombre	Teléfono Celular	Teléfono Casa	Dirección
CRTI	**Coordinador**	Primario	Director de TI	Víctor Melo	66712574	223-8674	Ave. A, San Felipe, Casa No. 32.
		Secundario	Subdirector de TI	Juan Rodríguez	64274379	537-7483	Edificio Vista del Mar, Ave. Balboa, Apto. 13B.
CIT	**Coordinador**	Primario					
		Secundario					
	Servidores y HW	Primario					
		Secundario					
	Controlador de dominio	Primario					
		Secundario					
	Soporte Técnico	Primario					
		Secundario					
	Comunicaciones	Primario					
		Secundario					
	Backup/Restore	Primario					
		Secundario					
ASE	**Asesor de Seguridad**	Primario					
		Secundario					

ANEXO F - Reporte de equipos evaluados.

Nombre del equipo	Código del equipo	Estado
<indicar el nombre del equipo evaluado>	<indicar el código del equipo>	<Indicar si el equipo evaluado se debe recuperar, comprar o arreglar>

<En caso de tener que realizarse compras de equipos producto de la evaluación debe adjuntarse este anexo al informe de compra>

Fecha: <indicar fecha de evaluación>

Evaluador: <indicar nombre de las persona que evaluó los equipos>